ACADEMY OF MILITARY-POLITICAL SCIENCES
OF UKRAINE

Yurii V. Semeniuk, Serhii P. Mokliak, Yurii M. Lysetskyi

THE NEW GEOMETRY OF INTERNATIONAL RELATIONS AND INTELLIGENCE ACTIVITIES

Scientific Monograph

Kyiv 2026

УДК 355. 40:007
М74

Recommended for publication by the Academic Council of the Academy of Military-Political Sciences of Ukraine (Minutes No. 4 dated March 18, 2026)

Authors:
Yurii V. Semeniuk – PhD in Political Sciences;
Serhii P. Mokliak – Doctor of Political Sciences, Professor;
Yurii M. Lysetskyi – Doctor of Engineering Sciences, Associate Professor.

Reviewers:
Valentyn V. Petrov – Doctor of Political Sciences, Associate Professor, Professor of the Department of Global and National Security of the Public Administration and Civil Service Educational and Scientific Institute of the Taras Shevchenko National University of Kyiv;
Mykhailo V. Koval – Doctor of Military Sciences, Head of the National Defense University of Ukraine.

Under the general editorship of Serhii P. Mokliak

Semeniuk, Y. V., Mokliak, S. P., Lysetskyi, Y. M. *The New Geometry of* M74 *International Relations and Intelligence Activities.* Ed. by S. P. Mokliak. Kyiv: Bykhun V. Y., 2026. 216 p.
ISBN 978-617-8553-05-0

The monograph is dedicated to the problem of the transformation of international relations and intelligence activities in the current context. The paper examines the geopolitical transformations of the modern world in the context of Russia's full-scale invasion of Ukraine. The new generation of Russian wars is assessed: key tendencies and ideas. It investigates the formation and development of Private Military Companies, their specifics and capabilities under conditions of destabilized international security. This work presents the concept of "intelligence activity" in modern conditions. The place and role of non-state actors in intelligence activities in the context of safeguarding national interests are considered.

The materials in the monograph will be useful to scientists, university teachers, postgraduate students, and professionals whose work is related to national security.

ISBN 978-617-8553-05-0

CONTENT

LIST OF ABBREVIATIONS AND DESIGNATIONS

A&ME	–	Armaments and Military Equipment
ADS	–	Air Defense Systems
AF	–	Air Forces
AFU	–	Armed Forces of Ukraine
AI	–	Artificial Intelligence
AntAc	–	Anti-Corruption Action Center (Ukraine)
ARPA-Ed	–	Advanced Research Project Agency for Education
ASEAN	–	Association of South-East Asian Nations
BDI	–	Behavioral Dynamics Institute
BRI	–	Belt and Road Initiative
BRICS	–	Brazil, Russia, India, China, South Africa
CA	–	Cambridge Analytica
CIS	–	Commonwealth of Independent States
CoE	–	Council of Europe
CSPG	–	China Security & Protection Group
CW	–	Conscientious War
DARPA	–	Defense Advanced Research Projects Agency
DPR	–	Donetsk People's Republic
DREAD	–	Department of Research, Exploitation, Analysis, and Development
DSEI	–	Defence and Security Equipment International
ECOWAS	–	The Economic Community of West African States
EU	–	European Union
EW	–	Electronic Warfare
FBI	–	Federal Bureau of Investigation
FTC	–	Federal Trade Commission
GARDA	–	Government Advant Research Development Agency

GEOMINT	–	Geospatial Intelligence
GF	–	Geopolitical Futures
GMW	–	Global Modern War
IA	–	Intelligence Agencies
IARPA	–	Intelligence Advanced Research Projects Activity
IC (U.S.)	–	U.S. Intelligence Community
IGOs	–	International Intergovernmental Organizations
INGOs	–	International Non-Governmental Organizations
ISIS	–	Islamic State of Iraq and the Levant
ITAR	–	International Traffic in Arms Regulations
K&R	–	Kidnap and ransom
LPR	–	Luhansk People's Republic
MAD	–	Mutually Assured Destruction
MASINT	–	Measurement and Signature Intelligence
MIA of Ukraine	–	Ministry of Internal Affairs of Ukraine
MM	–	Mass Media
MOS	–	Military Organization of the State
MW	–	Mental Warfare
NATO	–	North Atlantic Treaty Organization
Navy	–	Naval Forces
NDC	–	NATO Defense College
NESA	–	National Electronic Security Authority
NGOs	–	Non-Governmental Organizations
NIE	–	National Intelligence Estimates
NLP	–	Natural Language Processing
NPP	–	New Physical Principles
NSA	–	National Security Agency
NSA	–	National Security Agency
NWCC	–	NATO Warfighting Capstone Concept
OAS	–	Organization of American States
OSCE	–	Organization for Security and Co-operation in Europe
OSINT	–	Open Source Intelligence
OXFAM	–	Oxford Committee for Famine Relief
PGM	–	Precision-Guided Weapons

PLA – People's Liberation Army of China
PMC – Private Military Company
POA – Peace Operations Association»
PRC – People's Republic of China
PRC – Private Intelligence Company
PSC – Private Security Company
QUAD – Quad group of nations
RAND – Research and Development
RF – Russian Federation
RIA – Radio Intelligence Agency
RMCS – Robotic Military Complexes / Robotic Military Systems
SAS – Special Air Service
SC – Security Council
SCL – Strategic Communication Laboratories
SCO – Shanghai Cooperation Organization
SIGINT – Signals Intelligence
SMM – Social Media Marketing
TAG – The Arkin Group
TMO – Theater of Military Operations (Theater of War)
TTC – Trade and Technology Council
UAE – United Arab Emirates
UAVs – Unmanned Aerial Vehicles
UN – United Nations
USA – United States of America
USSR – Union of Soviet Socialist Republics
VUCA – Vision, Understanding, Creativity/Clarity, Agility
VUCA – Volatility, Uncertainty, Complexity, Ambiguity
AM – Additive Manufacturing

PREFACE

The contemporary geopolitical arena is witnessing an age of change, marked by the revival of established actors and the emergence of new state actors on the international scene.

The full-scale aggression of the Russian Federation (RF) against Ukraine is a telling token of the massive transformations in the world order. A bloodbath in the heart of Europe, a prospect that seemed improbable until very recently, given the humanitarian achievements of modern civilization and the political outlook of democratic countries, has become a reality.

A country that is a permanent member of the United Nations Security Council (UNSC) shows an utter contempt for the norms of international law, betting on military force and nuclear blackmail against the rest of the world. By relying on the sale of mineral resources as its primary source of revenue for the national budget, the RF issues primitive ultimatums to democratic countries.

All of this shapes the contours of the new world order, drawing a clear line between democratic Western civilization and autocratic Eastern. No alliances and allies are being made in this world, no mutual commitments, and old treaties can be unilaterally revised. Only big, powerful countries that take what they want and small, weak ones that are falling victim to such policies.

In other words, military force is gradually supplanting civilizational and global legal factors and is becoming the dominant force in the emerging world order.

Seeking to protect itself, each nation is rearming and placing strategic, geographic, and technological bets to survive and prevail in future confrontations. However, every one of these actions reinforces the sense of menace among adversaries, who in turn feel more insecure and brace for the worst, thereby making the situation appear even more threatening.

Particular emphasis is placed on the countries of the so-called Global South. The People's Republic of China's (PRC) geopolitical influence is one of the state's main global ambitions. Since Xi Jinping became General Secretary of the Communist Party of China in 2012, the country has departed from Deng Xiaoping's foreign policy, as expressed in his phrase "hide your strength, bide your time, keep a low profile." Instead, in 2014, the Chinese president gave a new definition of China's foreign policy: "seek achievements." In his new multipolar order, global institutions and norms will be backed by Chinese ideas of common security and economic development, Chinese values of state-defined political rights, and Chinese technologies.

In this "new world without order," the United States (USA) cannot remain on the sidelines. The understanding that stability and security in any region affect stability worldwide must become a key factor in resolving geopolitical issues. Cooperation, dialogue, and compliance with international law must be at the heart of any action on the international stage.

Therefore, today's international relations, the dynamics of geopolitical shifts, the growing intensity of information attacks and warfare call for a coordinated strategy to counter threats to global and national security.

INTRODUCTION

In today's global context, as geopolitical, geoeconomic, and sociocultural transformations and technological progress accelerate, the international arena is becoming increasingly complex and unpredictable. This dynamism gives rise to new challenges that, in turn, require deep understanding, adaptability, and immediate responses from countries around the world.

Current global trends create conditions for the rapid development of partnerships between state and non-state actors in world politics across various levels of international cooperation. Over the past decades, the number, diversity, scope, and scale of non-state actors' activities in international relations have grown significantly. These actors are gaining increasing influence over global processes, actively shaping modern political relations, defining the new contours of the international system, and playing a crucial role in addressing international security.

Emerging hybrid threats, changes in the nature of traditional ones, and, given the uncertainty, the increasing unpredictability of the future security environment – all these are new conditions in which Ukraine's intelligence agencies (IA) must operate, necessitating their adaptation, in particular through the introduction of new methods and means of operation.

SECTION I

GLOBAL GEOPOLITICAL TRANSFORMATIONS AMID FULL-SCALE RUSSIAN INVASION OF UKRAINE

1.1. Military Force as a Factor in Current Geopolitical Transformations

War is an inextricable part of human civilization. From the earliest historical records, the evidence of constant wars between groups fighting to conquer neighboring peoples and lands is abundant.

Nothing has changed in this regard in our time, as is evident, in particular, from the history and tragedies of World War II. The liberal world order that had risen from the ruins of that war resulted from a system of compromises between opposing ideologies – far from ideal, but nevertheless quite effective.

The system of multilateral agreements, conventions, and treaties on security, trade, and diplomatic relations, developed after World War II, arose in the midst of a continuous struggle between the ideologies, political, and economic interests of the so-called West, led by the United States, and the so-called East, represented by the USSR and a handful of its ideological satellites. Both sides acted within the post-war structure, recognizing the horror and futility of open aggression. With that in mind, the West mistakenly believed that the involvement of communist regimes in the global economic process would bring about their democratization.

An incorrect assessment of the Cold War's legacy and an inability to clearly explain the processes transpiring in the post-Soviet space in the early 1990s led to a series of flawed decisions by the West. Instead of creating a balanced security framework to prevent a new nuclear confrontation, a decision was made to reset relations with Russia and integrate it into multinational structures.

The start of the 21st century was marked by complex transformative processes driven by the challenges of globalization, the intensified role of ethnic and religious factors, radical shifts in the international environment, and changes in the security system.

The global community continues to view military force as one of the key tools for resolving foreign policy issues. World actors take decisions on the use of military force based on their own perceptions of national interests and the appropriateness of its use, even without a UN resolution.

The direct manifestations of military action can vary across several possible models of its objectification. At the same time, according to O. Panfilov, L. Petrova, M. Trebin, and others [1], the simplest scenario for a state to resort to military force, both on the international stage and within its own borders, continues to be the demonstration of the threat of force (overt – covert, real – conditional); armed violence remains a more complex form of military force – direct physical coercion of the opponent using means of armed struggle aiming at its destruction or desirable transformation and, accordingly, the achievement of one's own political goals.

Researchers note that, in modern conditions, the three most universal forms of power resources are economic, political, and military. Military power, compared to economic or political advantages, is the least adaptable to prompt conversion. However, its value lies in its role as a constant factor in relations, ensuring that all other factors are implemented. In peacetime, the force factor acts like a gravitational field: its effect on all processes is, at first glance, invisible yet decisive. Military force arises from the synthesis of relevant assets, a clearly defined goal, and an optimal model for organizing resources to achieve that goal, grounded in civilizational development. In this regard, the findings by O. Bodruk, which analyze the peculiarities of the formation of the factor of force in different countries of the world [2, 3], seem relevant. Based on the problem analysis, the author identifies several groups of countries with similar approaches to forming the military force.

The first group consists of developed European countries. They have completed the process of nation-building. In the global geopolitical space, they have long existed as sovereign entities. Well-developed democracies and market economies enable these states to truly represent the interests of the nation, individuals, and social or political groups. As a rule, such countries act as nation-states. Their military power issues focus on preventing external threats and challenges such as hybrid threats, terrorism, uncontrolled migration, organized crime, drug trafficking, etc.

The second group consists of countries where nation-building is not yet complete, but there are real opportunities to achieve national consolidation. Here, the state plays the primary role in nation-building. In this case, national goals are forward-looking, and military power is primarily directed toward the security of the state and its structural components. Only in specific cases does it extend to protecting other components of the social system. The security of this group of countries is mainly focused on internal problems: overcoming political instability and economic crisis; preventing separatism and conflicts on ethnic, political, or religious grounds; protecting territory, etc. These countries face external threats that require significant resources to maintain their military forces.

The third group includes multi-ethnic countries in Asia, Africa, and Latin America. They copied their state structures from former colonial powers; they lack democratic traditions, and their complex ethno-social structure creates enormous difficulties for progressive governments. Such states, especially in Africa and Asia, often become corrupt, ineffective, and delegitimized due to their inability to govern. In this case, there is every reason to talk about "the breakdown of the state" and see it as the main threat to the planet. In many cases, researchers note the actual absence of the state or the prolonged loss of state control over part of its territory. Numerous cases suggest the permanent coexistence of a weak central government and opposition armed groups control part of the country's territory so firmly that they are able to establish administrative bodies there. The economies of such countries and the institutions of state

power that are supposed to uphold the rule of law and order are in apparent decline.

In this context, the views of the US leadership on the use of military force in international relations are noteworthy. *On October 12, 2022, the US administration presented a new National Security Strategy of the United States of America [4].*

The document emphasizes that the US will not hesitate to use force to protect its national interests. However, the use of force must be based on clear, achievable goals, comply with values and laws, and be carried out with the consent of the American people.

Amid intensifying competition, the role of the military is **to maintain and gain warfighting advantages while limiting those of competitors.**

To achieve maximum effective deterrence of aggression, a new comprehensive approach is proposed: **integrated deterrence.**

On October 27, 2022, the Pentagon released the public component of the new US National Defense Strategy (hereinafter, the Strategy) [5].

The Strategy defines the following defense priorities: defending the homeland; deterring strategic attacks against the United States and its allies/partners; deterring aggression primarily from China and, to a lesser extent, Russia; and building a resilient Joint Force and defense ecosystem.

The main innovations of the Strategy are the concepts of integrated deterrence and peacetime campaigning. The United States plans to ensure the implementation of these priorities and goals precisely within the framework of these concepts. Coordination with allies and partners also plays an important role in implementing the Strategy's priorities.

The concept of integrated deterrence involves developing the U.S. armed forces' capabilities across all warfighting domains together with the U.S. network of alliances and partnerships. **Integrated deterrence calls for combining different types of deterrence to persuade the other side to abandon its aggressive intentions.** These are deterrence by denial, deterrence by resilience, and deter-

rence by cost imposition. The latter is based on the assumption that the enemy would suffer unacceptable losses if it attacked.

Deterrence by denial involves demonstrating to an adversary that it is impossible to capture and hold territory quickly or to achieve aggressive objectives rapidly. This type of deterrence complements deterrence by resilience, namely the ability to continue performing tasks despite sustaining a certain level of damage from an adversary (primarily to command-and-control systems). However, as the Strategy states, these types of deterrence may not be sufficient at times. Then deterrence is achieved through the ability to inflict unacceptable levels of damage, demonstrating the capacity to hit a wider range of targets. At the heart of such deterrence by the United States are its strategic nuclear arsenal and conventional long-range strike systems, offensive capabilities in cyberspace, the nonlinear application of existing capabilities (irregular warfare), support for third countries' defense, sanctions and export controls, and diplomatic measures.

In Russia's case, deterrence by denial and deterrence by resilience are emphasized. **By contrast, for Russia's immediate neighbors, the approach focuses on developing options for deterrence by inflicting unacceptable losses on Russia.** In the short term, this involves modernizing denial and access restriction capabilities, enhancing interoperability and resilience, and expanding intelligence sharing among NATO (North Atlantic Treaty Organization) allies and partners. In the long term, it entails strengthening the ability of NATO allies to conduct high-intensity warfare, while the United States concentrates on enabling functions such as intelligence and electronic warfare (EW), and air support.

The concept of peacetime campaigning aims to provide the U.S. armed forces with a response to adversaries' pressure-to-escalate tactics. Peacetime campaigning comprises military presence in priority regions of the world to undermine adversaries' confidence in their ability to achieve goals through pressure tactics. This practice of countering enables better preparedness should a crisis escalate into conflict, by improving situational awareness, enhancing interoperability, and expanding accessibility. The practice of

peacetime campaigning primarily against China and Russia would involve a direct US military presence in priority regions of Eurasia. In other cases, the US would rely on a network of alliances and partnerships.

The development of U.S. defense forces is presented as the foundation for maintaining and strengthening deterrence. Priority areas include sustaining information superiority through the integration, protection, and restoration of information-processing and decision-making systems; increasing the speed and precision of detection and strike capabilities; ensuring logistics and the sustainment of forces under conditions of active adversary countermeasures; and developing concepts and capabilities for the selective neutralization of weapons systems. The objective is to achieve an optimal combination of technological solutions and operational concepts that complicate an adversary's ability to project force. **In crises, the U.S. Department of Defense may also directly provide effective asymmetric capabilities to the most vulnerable allies and partners.**

In contemporary geopolitical competition, military power has increasingly assumed a central role, in part compensating for the inability of some states to generate effective soft power. In Russia's case, limited capacity to project influence via 21st-century toolkit (advanced technologies, innovation-driven economic growth, breakthroughs in space exploration, or other globally attractive development models) has contributed to a reliance on traditional instruments of power. These include pressure tactics through energy exports, coercive military force, and nuclear blackmail.

On April 25, 2005, in his address to the Russian Federal Assembly, Vladimir Putin called the collapse of the USSR "the greatest geopolitical catastrophe of the 20th century" and thus publicly justified future geopolitical revanchism with his nostalgia for the USSR.

On February 10, 2007, at the Munich Security Conference, Putin criticized the unipolarity of the world and the policies of the U.S. and NATO toward Russia: "For the modern world, a unipolar model is not only unacceptable, but also impossible." According to experts, this was the Kremlin leader's most radical foreign policy speech in

half a century, comparable to those of Soviet leader Nikita Khrushchev at meetings with U.S. representatives and from the UN podium. Putin's Munich speech was called the declaration of a second Cold War.

According to Ukrainian analyst M. Gonchar, the years 2007–2008 marked both the peak of global oil prices and the onset of the first global economic crisis of the 21st century, which originated in the United States and had worldwide repercussions. Against the backdrop of economic difficulties in the West and the heavy operational burden on the United States in Afghanistan and Iraq, the Putin regime benefited from rising revenues from Russian oil exports as well as from its ability to block certain NATO decisions, notably through the positions taken by European leaders such as Angela Merkel and Nicolas Sarkozy. President Putin signaled that "... if NATO provides a NATO membership action plan (MAP) to Georgia, Russia will recognize Abkhazia and South Ossetia based on the Kosovo precedent and thus create a buffer zone between NATO forces and its borders ... if Ukraine joins NATO, this state will simply cease to exist. That is, he actually threatened that Russia could begin tearing off Crimea and Eastern Ukraine." [6]

On February 20, 2008, G. Friedman clearly predicted the behavior of the Russian Federation: "...to annex Russian-friendly separatist regions on its borders — most notably the Georgian regions of Abkhazia and South Ossetia, and perhaps even eastern Ukraine and Crimea… Russia thus would argue that Kosovo's independence opens the door for Russia to shift its borders, too."

However, instead of penalizing Russia with sanctions for its invasion of Georgia, it was effectively rewarded with a policy of reset by the Obama administration. At the Munich Security Conference on February 7, 2009, U.S. Vice President Joe Biden articulated: "It is time — to paraphrase President Obama — it is time to press the reset button and to revisit the many areas where we can and should be working together with Russia." Moreover, on March 6, U.S. Secretary of State Hillary Clinton presented Russian Foreign Minister Sergey Lavrov with a symbolic red reset button. On the eve of the

meeting, on March 5, 2009, NATO foreign ministers decided to resume official dialogue with Russia within the framework of the NATO-Russia Council, even though Moscow had not implemented the August 12, 2008, ceasefire plan and had not withdrawn its troops from Georgian territory.

The NATO summit in Strasbourg-Cologne on April 3-4, 2009, revealed the Alliance's ambivalent position: on the one hand, it demanded the withdrawal of Russian troops from Georgia, and on the other, it cooperated with Russia on issues of missile defense, security in Central and Eastern Europe, Afghanistan, counterterrorism, etc.

In 2014–early 2022, Ukraine found itself at the epicenter of a new phase of global confrontation between the West and Russia. At its core was the Putin regime's attempt to achieve "geostrategic revenge" for the USSR's defeat in the Cold War and restore Russia's status as a world power. Despite Russia's formal recognition of Ukraine's independence and sovereignty, Moscow viewed our state as an artificial entity that fell within the Kremlin's "special interests" and was a key part of the geopolitical project of the "Russian world." During eight years of low-intensity conflict, Russia turned Donbas into a "gray zone" that served as a geostrategic springboard for military and political pressure on Kyiv and a potential "safeguard" against Ukraine's accession to NATO and the European Union (EU).

Unable to achieve his goals through hybrid warfare in 2021, Putin decided to move on to the next phase of his aggression against Ukraine, using the full force of his military. Under the guise of military exercises and maneuvers, Russia concentrated a large group of troops and equipment on the border with Ukraine, which threatened to escalate hostilities and caused a wide international response. Russia's comprehensive military-political and purely military preparations for the invasion of Ukraine began no later than the spring of 2021 under the guise of numerous exercises, including on the territory of Belarus. Negotiations between Russia and the West on a draft "treaty" on European security and "security guarantees" for Russia served as a political and diplomatic cover for these preparations.

The full-scale military aggression against Ukraine, launched by Russia on February 24, 2022, brought an end to more than half a century of peaceful coexistence between states on the European continent, founded on mutual recognition of sovereignty and territorial integrity under international law.

Experts at the Razumkov Center assessed how this war exposed significant challenges in global and regional security systems [7]. We will dive into these in more detail.

1. The UN Security Council's veto practice hinders, and, in the worst case, prevents decision-making on conflict resolution when it directly or indirectly affects the interests of the Council's permanent members. Unacceptable is the fact that in the Russian-Ukrainian war, Russia, as a permanent member of the Security Council and a recognized aggressor, is blocking decisions related to the resolution of the conflict. The latter contradicts common sense and calls for immediate reform of the UN.

2. The UN security system has demonstrated limited political will and institutional capacity to resolve armed conflicts, ensure compliance with international norms, and commitments. Owing to the absence of sustained political will, financial and military-technical constraints, and the extensive use of veto, the peace enforcement mechanisms envisaged in the UN Charter have effectively disappeared from the UN Security Council's operational toolkit. In practice, the organization relies on less coercive instruments, such as peacekeeping and peacebuilding (often described as "Chapter VI+" or "Chapter VII–" operations). Such a preference of the United Nations and other security organizations for approaches that sidestep complex problems often results in deferring rather than resolving underlying conflicts. The emphasis on ceasefire as a core element of settlement often prolongs conflict in a "frozen" state and leads to its subsequent re-escalation. The freezing of a conflict in eastern Ukraine following 2014, foreseeably overgrowing into a war of aggression by the Russian Federation against Ukraine, is a striking example.

3. The West as a whole, its security institutions, and the national security systems of the vast majority of Western states proved

unprepared for Russia's full-scale aggression, which brought the world to the brink of World War III. Conversely, the entire world was surprised by how a powerful aggressor could not only face resistance but also suffer defeat in a confrontation with a country whose people and government are consolidated in the cause of defending freedom and territorial integrity. Moreover, if Ukraine had not stopped Russia's blitzkrieg, the West might not have recovered or would at least have suffered significant damage to its image after such a brazen and aggressive "raising of the stakes" by the Kremlin. The initial phase of Russia's war against Ukraine, the Russian Federation's ultimatums to NATO, and its latest nuclear blackmail of the U.S. and European countries demonstrated the need for collective and national security systems to include early warning mechanisms, threat prevention, adequate and effective responses not only to actual aggression, but also to threats of aggression. The importance of force availability and reserves, as well as means and resources, has increased, alongside the need for effective, well-developed employment mechanisms, readiness to deploy, and the provision of assistance to allies and partners.

4. The degree of hybridity in international conflicts and crises is increasing, characterized by the use of non-traditional instruments of war, such as energy resources, political corruption, aggressive propaganda, and cyber weapons. Recently, food has been added to this list. The use of these weapons by the aggressor state reveals it as a deceitful and cruel actor. Currently, the main areas and forms of use of these types of weaponry by Russia are as follows:

- pressure on the West, attempting to discredit it by appealing to the colonial past of the countries in Asia and Africa, highlighting the inequality between the North and South, and spreading misinformation about the origins of COVID-19 and the unfair distribution of vaccines;
- undermining European solidarity by fueling the energy crisis and discontent among the populations of European countries on the eve of and during the winter season;
- hopes for a decline in the resilience of EU countries, deflecting attention from the war in Ukraine by forcing them to respond to

waves of migration triggered by grain shortages, the supply of which from Ukrainian ports has been blocked by Russia itself;
- strengthening its position on the international stage by contrasting Russia with the "decaying" West;
- mitigating the effects of sanctions by encouraging individual countries to refrain from participation and the introduction of "gray" and smuggled supply chains for goods and technologies needed by the Russian defense industry;
- weakening Ukraine's economic potential and blocking Western aid.

5. The war has highlighted the shortcomings in the effectiveness of existing economic and security alliances. The key issues here are mistakes in risk assessment, an inability to prevent crises, delayed response to them, and individual allies' careless attitude toward resource needs. In this context, doomsday predictions are often heard about the end of the globalization era, the era of large alliances, and the transition of initiative from centralized to network structures, in the form of autonomous regional and subregional unions, alliances, and coalitions. There are indeed indications of such processes; however, the focus is on finding ways to achieve internal solidarity and stability within existing intergovernmental alliances and coalitions. Examples include the following:

- The Nordic Defence Cooperation, already available in Europe, the Visegrád Group (V4), the Lublin Triangle, and the Three Seas Initiative (3SI or TSI);
- Boris Johnson's initiative on establishing outside the EU under the auspices of Great Britain of a new military, political, and economic union, participated by Ukraine, Poland, Estonia, Latvia, Lithuania, and Türkiye;
- Emmanuel Macron's idea, already starting to be implemented, to create the European Political Community involving, apart from all EU members, also all Western Balkans' countries, Ukraine, and Moldova;
- Coalitions of states that emerged in relation to aid for Ukraine to counter Russian aggression (the Ramstein and Copenhagen

processes). That means this war has become an indicator of the neo-empire policies of the Kremlin. The Russian authorities consider the war in Ukraine merely as part of the big game, targeting to achieve world leadership. As proof of this, further Russian actions in the Middle East and on the African Continent.

In October 2023, the conflict between Israel and HAMAS – an Islamist organization that has been in control of the Gaza Strip since 2006 – escalated. During its attack on the territory under control of Israel, HAMAS killed over 1,400 Israelis and citizens of other countries, more than 5,000 people were injured, and around 250 people were taken hostage. This large-scale attack led to Israel being forced to declare war and carry out the "Lethal Response Operation." The terrorist actions of HAMAS groups received support from a number of Arab countries, such as Qatar, Iraq, Iran, Türkiye, Kuwait, Syria, Jordan, Tunisia, Algeria, and Yemen, as well as from Afghanistan and North Korea. On the other hand, in this conflict, Israel gained support from most European countries, including Ukraine. The United States has also announced full diplomatic and military support for the Israeli armed forces. The EU has issued a statement condemning the numerous and indiscriminate attacks by HAMAS and calling for an immediate stop to the violence. If we analyze the list of countries that support one or another side in this armed confrontation, we can conclude that almost the entire Arab world is decisively determined to defend its interests with the use of arms and of any force to achieve its goals.

Another sign that this conflict transcends Israel and Palestine is the fact that on October 26, 2023, Hamas leaders arrived in Moscow for a meeting with high-ranking officials. The Israeli Foreign Ministry condemned the decision to invite Hamas members to Moscow, calling it an "act of support of terrorism" and urging Russia to expel the delegation from Moscow. However, the Kremlin has been slow to declare its intentions regarding support for Israel in this conflict. Moreover, the Kremlin has officially condemned Israel's strikes on the Gaza Strip, and the Hamas leadership itself has repeatedly em-

phasized its close cooperation with the Russian leadership. In this case, there may be several reasons for such an alliance, the main and most important one is the Kremlin's hope for a reduction in military aid to Ukraine in its war for independence against Russia.

Russian influence in Africa became a topic of discussion after 2014, when the country faced its first sanctions. The continent proved particularly valuable to Russia's defense sector, as it has been cut off from many contracts worldwide. Before 2013, the share of Russian weapons in Africa fluctuated between 11% and 25%, but after 2017 it grew to over 40%. As of 2020, half of the weapons imported to Africa came from Russia.

Energy is another lever for Russia's influence in Africa. Nearly 600 million Africans lack permanent access to electricity. Droughts and other climatic disasters further exacerbate the situation. In 2019, Algeria, Ghana, Zambia, Nigeria, and Rwanda decided to bet on Russian nuclear energy. The terrorist country promised to build a few nuclear power plants for them over time.

The 2023 Russia-Africa Summit underlined Moscow's desire to expand its economic presence, targeting agriculture, mining, and energy, aiming to double trade figures by 2030.

Russia and its state-owned enterprises - "Rosatom" in the energy sector, and "Rusal" in the mining industry - are engaging in projects that, while not large in terms of investment, are of significant political and strategic importance.

These projects often involve critically important raw materials. Above all, uranium is key to nuclear energy and could give Russia significant control over these resources. For example, "Rosatom" actively expands its uranium reserves, partly through the purchase of a project in Tanzania for $1.15 billion [8].

Russian control extends beyond raw material to the entire nuclear fuel cycle. While Russia is a relatively small producer of raw uranium, it accounts for a significant share of global uranium processing and enrichment infrastructure, approximately 40% and 46%, respectively. These capabilities are critical because they enable the conversion of raw uranium into nuclear reactor fuel.

In addition, Russia dominates the export of nuclear power plants. Between 2012 and 2021, it initiated the construction of 19 nuclear reactors, 15 of which were located outside Russia. These figures are far superior to those of any other country during the same period.

Although Russia's economic presence in Africa is not as extensive as China's, its role in supplying strategic goods and military equipment to African countries is a multilayered challenge. Should Russia secure control over the supply of critical resources such as lithium or uranium, it could create dependencies, shape market prices, and use them for political leverage, as it currently does in other regions.

Potential risks of such activities are enormous. A foreign state's control over critical resources, especially when aggressive, affects national sovereignty and poses a global strategic challenge, as these resources are vital to the "green" energy transition and technological development worldwide.

After all, Russia's modest economic involvement in Africa may not be of great importance to Moscow. Russia's real motives for engaging with Africa lie in promoting its geostrategic interests, in securing a foothold in the Mediterranean Sea on NATO's southern border, displacing Western influence, and promoting Russia's worldview. In other words, Africa is a stepping stone for Russia's broader strategic goals [9]

While Russia welcomes the increase in trade opportunities with Africa, the political benefits are the most appealing. Holding 54 votes in the UN General Assembly, Africa is an attractive "target" for Russia to justify its military aggression and violations of international law.

In addition, Russia's most excellent source of influence in Africa comes from unconventional, asymmetric instruments such as co-opting elites, spreading misinformation, interfering in elections, deploying the Wagner Group, and trading weapons for resources.

Starting in 2018, when Wagner mercenaries arrived in the Central African Republic, Moscow has been gradually increasing its presence and influence in Africa. In particular, in the Sahel region, which stretches from the Atlantic Ocean to the Red

Sea, after military coups in Burkina Faso, Mali, and Niger, the juntas that seized power are curtailing military and political cooperation with the United States and France and strengthening relations with Russia.

At the same time, experts believe [10–12] that, for China, which has acquired and controls much more of Africa than the United States and France, **Russia's penetration into Africa is beneficial because it weakens U.S. influence. The competition that sometimes arises between Chinese and Russian companies is not critical,** as the Chinese focus on participating in the development of the continent's natural resources and on providing loans to African states. At the same time, the Russians prioritize the military and military-technical domains.

In their turn, the U.S. is officially discussing its readiness for possible simultaneous wars with Russia and China. In particular, the 2023 America's Congressional Commission's Final Report on Strategic Posture [13] states that the U.S. and its allies must be prepared to deter and defeat both adversaries simultaneously. It also states that the international order "is under threat from the Chinese and Russian authoritarian regimes." The authors of the report believe that the Chinese and Russian threats will intensify in 2027–2035. Therefore, "Decisions need to be made now in order for the nation to be prepared."

They also recommend fully funding a 30-year program to modernize the U.S. nuclear arsenal by 2046, estimated at $400 billion in 2017.

The recommendations include deploying additional tactical nuclear weapons in Asia and Europe, as well as developing plans to utilize some or all of the United States' reserve nuclear warheads. Additionally, it advised increasing the production of B-21 strategic bombers and new Columbia-class nuclear submarines.

In March 2025, U.S. Secretary of Defense Pete Hegseth signed a document titled "Interim National Defense Strategic Guidance." This document outlines the implementation of President Donald Trump's strategy to prepare the U.S. for a potential conflict with China and to safeguard national security. It emphasizes the protection of key strategic locations such as Greenland and the Panama Canal.

Aside from reallocating military resources toward the Indo-Pacific region, the memo also assigns new tasks to the U.S. Department of Defense.

The Hegseth document identifies a potential Chinese invasion of Taiwan as a primary threat, one that surpasses other challenges. As a result, the structure and resources of the U.S. armed forces will primarily focus on countering Beijing.

Additionally, Washington intends to pressure its allies in Europe, the Middle East, and East Asia to increase their defense spending and take a more active role in deterring threats from Russia, North Korea, and Iran.

The document also notes that the Pentagon will modify its approach to counterterrorism operations. Emphasis will be placed on combating groups that pose a direct threat to the U.S., while reducing attention to terrorist networks that operate locally without international ambitions. "China is the Department's sole pacing threat, and denial of a Chinese fait accompli seizure of Taiwan — while simultaneously defending the US homeland is the Department's sole pacing scenario," Hegseth wrote in the memo.

On 1 May 2025, U.S. Secretary of Defense Pete Hegseth signed a memorandum initiating the development of a new U.S. National Security Strategy. According to a press release issued by the U.S. Department of Defense, the Department's components were tasked with drafting a revised strategy that reflects President Trump's campaign priorities, notably the principles of "America First" and "Peace through Strength" [14].

1.2. Global South as a Mega Subject of the Contemporary Geopolitical Game

Russia's full-scale invasion of Ukraine has profoundly changed the perception of the security situation in the world at the global, regional, and subregional levels. The picture of the current world stands in stark contrast to that of the latter half of the 20th century,

when the Cold War between the geostrategic East and West centered more on international statics than dynamics.

As Serhiy Korsunsky, Ukraine's Ambassador Extraordinary and Plenipotentiary to Japan, aptly pointed out: "The current state of geopolitics can be described by a formula that, although complex, is understandable to those in the know. The number of countries willing to contribute to the foundation of a new world order is greater than or equal to the number of potential mediators for negotiations with Russia to end the war. Yet, it is significantly smaller than the number of domestic experts on Southeast Asia who have never been there yet feel they fully understand the situation. In defense of the latter, it is important to acknowledge that it is indeed challenging to comprehend the contradictory actions of some of the most significant countries in the region." [15]

Consequently, the significant role of East and Southeast Asia in global politics and economics is an axiom of contemporary geopolitics. Globalization and the Internet have virtually eliminated the possibility of isolationism and removed the barriers of distance from conflict zones, ensuring that developments in Europe now have a direct resonance in Asia. Russians have been promoting their interests in India and China for decades, supplying weapons to the Indo-Pacific region, opening educational centers in many countries, and forming an expert community. Myths about "the great Russian culture," "the Soviet Union's and later, Russia's struggle against imperialism and colonialism," the aggressive propagation of useful and fabricated historical narratives, as well as outright political corruption, are just a few of many tools Moscow has used to shape public opinion and political circles.

Of course, the Kremlin did not expect a strong and decisive Western response to its invasion. Yet the Russian invasion brought about extraordinary unity and joint action across the liberal-democratic world. Western countries have been coordinating to implement an unprecedented set of economic sanctions against Russia.

On March 2, 2022, the UN General Assembly adopted its first resolution of the eleventh emergency special session (UN General Assembly Resolution ES-11/1) [16]. The document deplores the

Russian invasion of Ukraine and demands the complete withdrawal of Russian troops and the reversal of the decision to recognize the self-proclaimed Donetsk and Luhansk People's Republics. The resolution was adopted with 141 votes in favor, 5 against, 35 abstentions, and 12 absentees.

In turn, most of the "non-European" countries that voted to condemn Russia's aggression in March 2022 did not impose sanctions against it.

In total, in a series of UN votes since the start of the war, around 40 states, representing almost half of the world's population, regularly abstained or voted against motions condemning the Russian invasion.

In the opinion of experts from the authoritative magazine *Foreign Affairs*, disputes are not driven by disagreements over the war in Ukraine. Still, they are instead a symptom of a broader syndrome: anger over the West's double standards and frustration with stalled efforts to reform the international system. For example, some of them argue that the rules-based international order does not serve Africa's interests. Instead, this order has preserved the status quo, with major world powers - both Western and Eastern - continuing their dominance. China, France, Russia, the United Kingdom, and the United States have significantly influenced African countries through the UN Security Council, leaving African governments as mere bystanders in their own affairs.

The distinguished Indian diplomat Shivshankar Menon put the point sharply in Foreign Affairs in early 2024 when he wrote, "Alienated and resentful, many developing countries see the war in Ukraine and the West's rivalry with China as distracting from urgent issues such as debt, climate change, and the effects of the pandemic."[18]

We can therefore state that Realpolitik has played a role in shaping the positions of certain countries on the Ukraine conflict. India has traditionally been dependent on Russia for military supplies. The Wagner Private Military Company (PMC) has worked with governments in western and central Africa to support their regimes' security

and survival. And China, one of Russia's principal sources of support, is the largest trading partner of more than 120 countries.

In recent years, the so-called Global South has emerged as a meaningful factor in contemporary geopolitical processes. Currently, there is no single entity perceived to represent the Global South as a whole. The BRICS group (Brazil, Russia, India, China, and South Africa) is eager to lead this coalition, while the Shanghai Cooperation Organization (SCO) is another potential candidate for this role.

Analysis indicates that when people refer to the Global South, they do so from their own perspectives. For some, it denotes a collection of countries with a history of colonialism; for others, a diverse array of developing nations or at least members of the Non-Aligned Movement or "The Group of 77." There is no definitive list of countries considered part of the Global South, and none of the definitions provided are exhaustive or entirely clear.

The concept of dividing the world into North and South originated during the Cold War, a time when the globe was split into two opposing camps: the Eastern Bloc, led by the USSR, and the Western Bloc, guided by the United States and Western European nations. This division gave rise to a third category: countries that chose not to align with either camp.

The term "Global South" was coined by American political expert Carl Oglesby. In one of his articles, he argued that the Vietnam War marked the end of the era in which the North dominated the South. In this context, "North" referred to world empires and metropolises, while "Global South" described the colonial world. During the 1960s, former colonies of (mostly) European countries were often labeled as "Third World." This classification implied that countries in the "First World" were the most developed democracies with market economies, socialist countries belonged to the "Second World," and all other countries were part of the "Third World." In other words, countries that cannot be classified as belonging to any of the above categories.

This classification carried a clear discriminatory undertone, reflecting a bias toward "first-world" countries. Most of these countries

had been former colonies and, after gaining independence, were not always quick to navigate the complexities of international relations and did not align with either camp. Since this phrasing evoked associations with the term "third-rate," it came to be considered less appropriate. Consequently, since 1991 (when the "second world" ceased to exist), the term "Global South" gained wider use.

In 1980, a commission headed by former Chancellor of the Federal Republic of Germany Willy Brandt published a report. The commission noted a significant gap in economic development across countries worldwide. The so-called Brandt line demonstrated this division. This line spans the planet at 30° north latitude, running between North and Central America, northern Africa, the Middle East, and most of East Asia. The line then descends southward, indicating that Japan, Australia, and New Zealand are part of the Global North [19].

In geographical terms, 'Global South' describes 32 countries located below the equator (in the Southern Hemisphere), as opposed to the 54 countries located north of it. However, the term is often mistakenly used as a short form for the global majority, even though most of the world's population lives above the equator (and most of the world's landmass lies there). For instance, we frequently hear that India, the world's most populous country, and China, the second-most populous, are vying for leadership in the Global South. To this end, both countries have recently held diplomatic conferences. However, both are located in the Northern Hemisphere.

In addition, if we consider the geographical component, we can use the World Bank's definition, which includes middle-income countries in Africa, Asia, Oceania, Latin America, and the Caribbean. Not all countries in the south belong to the Global South - for example, Australia and New Zealand are omitted. However, the boundaries of the south are quite arbitrary, and some experts believe that Turkey, for example, is part of it.

Therefore, this term is more of a political slogan than an accurate description of the world. In this sense, it has gained popularity as a euphemism to replace less acceptable terms.

In contemporary geopolitics, revisionist states aiming for a new redivision of the world are particularly exploiting the concept of the Global South. China and Russia, for example, aspire to represent the interests of a fictitious association of countries. Aware of its political bankruptcy, Russia has given this association another name: **"the global majority,"** which, like all previous versions, lacks both definition and classification. Judging by the voting results on UN General Assembly resolutions, Russia is in the minority. In contrast, if we consider including the world's most populous countries, China and India, which, for various reasons, are members of both BRICS and the SCO, and both are claiming leadership over the interests of the Global South, one must first ask these countries whether they agree with Russia's claim to be on par with them.

The Global South encompasses a highly diverse group of countries. It includes states with near-perfect democratic indicators as well as overt dictator states. Part of the Global South countries condemned Russia's invasion of Ukraine, however numerous states adopted a neutral stance, or rather, **the stance of "not expressing any stance."**

South Africa is a staunch fighter for the rights of the Global South and a member of BRICS. The Africa Wealth Report 2024 by Henley & Partners shows that at the end of 2023, the country had 37,400 USD millionaires, 102 multimillionaires, and five billionaires [20]. This country ranks first in the Swiss bank UBS's "inequality index," with a score of 82 out of 100, an increase of 17.7% from 2008. Johannesburg alone is home to 12,300 millionaires and two billionaires.

Brazil ranks second on the inequality index, with **India** in fourth place. **The United States,** which faces challenges from BRICS, ranks honorable third. Among the countries of the Global South, **Egypt, Nigeria, Kenya, Morocco, Mauritius, Algeria, Ghana, Ethiopia, and Namibia** are leading the continent in the number of dollar millionaires. Forecasts indicate an expected 80% increase in their numbers over the next decade.

According to an OXFAM report **(Oxford Committee for Famine Relief)**, traditionally delivered in Davos, Africa's richest 1% owns nearly half of the continent's wealth. The combined wealth of the seven richest people is $52 billion, exceeding the income of 700 million Africans. Zimbabwe's only billionaire has increased his wealth by 40% since 2020, while Africa's richest man, a Nigerian, has a cement monopoly and has been paying 1% tax on his profits for 15 years.

Interestingly, OXFAM estimates that **African countries annually face a $200 billion shortfall in tax revenue due to various evasion schemes employed by major national and international corporations.** Meanwhile, corporate taxes **are the primary source of funding for social programs and budget formation for African states.** Overall, these issues are not specific to Africa or the Global South and are global in nature. Five of the world's wealthiest people have doubled their wealth over the past three years, while the incomes of 5 billion people have declined during the same period [21]. **13.5% of India's population lives on $15 per month, with a per capita GDP** (gross domestic product) **of slightly over $2,000.** At the same time, in July 2024, the media reported on a three-day celebration of Anant Ambani's wedding, the son of the richest man in India and Asia. By various estimates, the lavish event's expenses will amount to $350 million. Not only the prime minister of Asia's largest democracy, Narendra Modi, members of the government and parliament, were invited to the wedding, but also Mark Zuckerberg, Bill Gates, Hillary Clinton, Tony Blair, Boris Johnson, the Kardashian sisters, the Beckhams, Trump's daughter Ivanka, and many others [22].

According to a study by Humboldt University of Berlin, the "Global South" was mentioned about 20 times in publications in 2004. By 2014, there were hundreds of references.

The struggle for the Global South has been ongoing and intensified since the emergence of new states in Africa, Asia, and the Middle East following the collapse of the colonial system in the 1950s and 1960s.

Lately, this focus has only gotten stronger. Most of the world's population lives in the Global South. Furthermore, demographic trends suggest that in 25 years, one in five people on Earth will be African. Geographical and climate factors, migration security - all these issues mean that the Global North cannot ignore what is happening here.

Additionally, Ihor Semyvolos observes that the increased attention to the South coincides with a certain crisis in the West, whose long-standing active control over this territory is now waning. A void is emerging in these regions, which other states, notably China and India, are trying to fill [23].

The renowned Indian analyst C. Raja Mohan remarked: "Three summits this week — one in Davos, Switzerland, and the other two (NAM and G77) in Kampala, Uganda — point to the shifting terrain of global politics in 2024. The world's rich and powerful in Davos and the underprivileged in Kampala have a shared problem — dealing with structural changes in the international system. The old slogans — on globalism in Davos and collectivism of the Global South in Kampala — are no longer credible or sustainable." The summits, according to him, also underscored the contrast between India's and China's agendas. The annual gathering in Davos was tempered by the recognition that renewed great-power conflict and economic nationalism have upended the apple cart of globalization. The back-to-back summits in Kampala revealed that the renewed political euphoria about the Global South is insufficient to deal with the challenges and opportunities of the changing world order [24]. In other words, publicly available data indicate **a particular discrepancy between the ideological image of victims of the colonial past and the practical interests of the business elite of the "southerners."**

However, in light of the events Ukraine and the whole world are facing in connection with Russia's full-scale armed aggression, we should talk about the obvious political crisis in modern international relations and the importance of involving the countries of the Global South in discussions on the international agenda.

To be successful in this endeavor, we must approach each of these countries individually, for there is no single Global South entity. The partners are either already on our side or still need to be persuaded to join us.

The majority of Global South states choose to present their **position on the Russian-Ukrainian war as neutral.** Below are the key reasons behind these considerations:

- General anti-American sentiment in certain countries, though that does not automatically make them pro-Russian;The perception of the Russian Federation as an anti-imperialist power, the ideological successor to the USSR, and, respectively, the comprehension of most Western countries supporting Ukraine as imperialist states associated with the dictate and colonial past.
- The refusal to recognize Ukraine's struggle as an anti-colonial, stemming from several stereotypical beliefs. One such belief is that a "white country cannot be a colony." Additionally, there is a common association of Ukraine with Europe, that has historically been seen as a colonizer.
- Simultaneous dependency on Western financial aid and promises of financial aid or existing contracts with the Russian Federation.
- The history of the affiliation with the non-aligned movement.

In some countries, they express confusion about **how conditions for ending the conflict can be established without the involvement of the opposing party, Russia, in the negotiations.** In other words, members point to the lack of clarity in the initiative's format and purpose. Those presenting themselves as neutral express reservations, arguing that the current meetings aim at forming the position of one "side" (Ukraine and the West) against the other (Russia). Accordingly, their participation in meetings dedicated to Ukraine's "peace formula" will be seen as siding with Ukraine in the conflict.

Another important source of confusion among countries in the so-called Global South is the question of **why Ukraine's issues should concern them at all** and require their involvement in resolving a conflict so distant from them. Russia's extensive diplomatic and

propaganda campaign promoting false narratives on the so-called "roots of the war," the Ukrainian refugee issue, factors behind the halt in grain exports, and so on, has further contributed to this attitude. However, domestic debates on the topic often include assertions that Ukraine has never shown interest in its problems, suggesting that there are no grounds for solidarity.

Given the low literacy levels in the Global South, it is safe to say that, at best, they view Ukraine as a former Soviet republic. Moreover, their knowledge of Ukraine's recent history is often limited to the version presented by Russian propaganda. However, the attitudes of the elites in these countries tend to play a greater role, and, as we know, elites tend to think more pragmatically than in a value-based manner. Russian propaganda portrays the Global South as, at the very least, sympathetic states, if not allies.

1.3. Strategic Wartime Challenges: Objectives and Priorities

The war in Ukraine has accelerated global systemic processes, creating conditions of heightened uncertainty and unpredictability and, consequently, increasing anxiety among individual actors. These dynamics significantly complicate forecasting, the formulation of strategic and tactical priorities, and the coordination of cooperative efforts among states within frameworks designed to address the ongoing crisis.

The global transformations currently taking place extend beyond the realms of security and ideological confrontation. They also encompass the emergence of a new economic model that, without exaggeration, will shape humanity's future trajectory.

The international community must find a new model for its functioning while simultaneously addressing current political and economic challenges. The West, as the leading civilization, is in a crisis today. Although liberal democracies have succeeded in expanding "Greater Europe" by including post-socialist states, this process has not advanced beyond that point.

Former U.S. National Security Advisor Herbert McMaster described the key lessons of Russia's invasion of Ukraine as follows [25]:

First, the renewed invasion of Ukraine in February 2022 exposed the extent to which many policymakers in the free world remain attached to overly optimistic visions of the post–Cold War international order. Among these was the assumption that the history process would inevitably ensure the dominance of free and open democratic societies over closed authoritarian systems. Western policymakers assumed that the great powers competition had become a relic of the past. However, Chinese President Xi Jinping and Russian President Vladimir Putin shared a different view. The joint statement by the two leaders on the eve of the Beijing Olympics - despite containing false claims, persistent misrepresentation of facts, and Orwellian reality distortion - nevertheless conveyed a clear message. They signaled a challenge to democracies for global leadership, portraying them as divided, weakened, and in decline. The key clear conclusion follows from the assessment: allies and like-minded partners across the free world must identify new and more effective ways to counter Russia and China.

Second, the West realized that the triangular diplomacy employed by U.S. President Richard Nixon and U.S. Secretary of State Henry Kissinger in the 1970s, seeking to make U.S. bilateral relations with the USSR and China tighter, than the relations between these two countries, was simply impossible in a world where two revanchist powers had sworn that "friendship between the two states has no limits." China supported this vow, proclaimed in the run-up to the 2022 Olympic Games, through its odious "wolf warrior diplomacy," deliberately amplified Kremlin disinformation, and mitigated the financial and economic impacts of sanctions imposed by most of the free world against Russia. The idea of China and Russia counterbalancing each other is appealing, yet our adversaries have taken joint actions against the free world. The two countries rotate their roles in conflicts everywhere, from Syria to Pakistan, from Northeast Asia to the UN chambers, acting both as "arsonists and the firefight-

ers." Therefore, we should not make a distinction between Xi and Putin. The free world should view the two dictators as one. Not only because they are equally dangerous, but also because the benefits of the Russia-China partnership are amplified by their ability to support each other in their efforts to confuse, disrupt, coerce, and sabotage.

Third, Russian aggression and Ukrainian courage show that although war is not a desirable way to resolve disputes, it can be the only way to prevent another party from resolving them for you. To paraphrase British philosopher and religious thinker Gilbert Keith Chesterton, the necessity to strengthen collective defense and restore the policy of deterrence to prepare for a response to aggression is now overdue. The US, NATO countries, and similar-minded states such as Japan must not only enhance their own military capabilities without delay, but also help strengthen Taiwan's defenses, bearing in mind what could have been done before February 24, 2022, to help Ukraine prevent a new Russian invasion.

Fourth, relying on autocratic regimes as a source of energy supplies is a fatal mistake. For Germany, the shift to non-renewable energy sources, combined with the abandonment of nuclear power, was a step into the abyss of Russia's "embrace." Germany's dependence on Russian oil and gas weakened its immediate response to Russia's renewed brutal invasion of Ukraine at the initial stage, leading to increased coal burning and carbon emissions to keep its homes lit. Therefore, we conclude the need to establish new policies that combine energy and national security with policies to reduce carbon emissions.

Fifth, even sporadic disruptions to supply chains controlled by aggressors undermine sovereignty and hamper the ability to respond to aggression. Examples include not only Europe's dependence on Russian oil and gas, but also India's dependence on Russian weapons. For this reason, Xi Jinping is building a "dual circulation" economy that, in one respect, is less vulnerable to foreign markets, finance, and technology, and, in another, increases other countries' dependency on Chinese goods, components, and raw materials. The country is working to dominate critical supply chains for the clean energy transition.

In this way, the Russian-Ukrainian war has become a totality that challenges the current way of globalization. And now Ukraine has become a factor in determining a number of global developmental trends [26, 27].

First, the globalized world we live in has become a zone of constant confrontation between Russia and the West. The war has brought Western countries together in their opposition to neo-totalitarian Russia.

Second, Ukraine has become a kind of test for the West - particularly for Europe's ability to rediscover and fulfill its civilizational mission and to develop an active, forward-looking foreign policy. There is a growing understanding of the Euro-Atlantic community's role in Ukraine's victory. We are backed in our pursuit of a dignity-based peace by the democratic world, above all, the Euro-Atlantic civilizational community. Transatlantic cooperation has intensified since Russia invaded Ukraine. It is also noteworthy that NATO has expanded on Russia's doorstep: Sweden and Finland have abandoned decades of neutrality and become full members of the Alliance.

Third, Ukrainian civilizational agency is being revived and developed in the Euro-Atlantic geopolitical space. The world has recognized that the Ukrainian people belong to the Euro-Atlantic civilizational community. Ukraine has proven its readiness to leave behind the post-Soviet state and a gray intermediate zone, choosing a European trajectory for its development. In reality, we have moved away from the "Russian world" and have already been accepted into Europe.

Fourth, Russia's invasion of Ukraine has revealed Russia's departure from the European path and its return to the eastward course of its history. In particular, the current state and trends in the ethnic and demographic structure of Russian society provide a strong incentive for Russian elites to seek partnerships in the Muslim world and to cooperate with China, etc.

Fifth, the Russian-Ukrainian war has brought to light a fact of incredible historical significance: all lines of historical confrontation between Russia and Europe run through the Ukrainian cultural realm.

We are now witnessing the demise of the Russian ideological paradigm, previously partially adopted by the West: Ukraine, within it, was assigned a marginal role of a cultural province in the "Russian world." Today, interest in Ukraine is growing at an imperative rate, and we must meet the demand. That is why it is necessary to develop and present the very concept of Ukrainian culture and Ukraine's role in European history.

Sixth, there is a growing understanding that Russia's war against Ukraine is existential and ideological in nature. It is not just a war for interests or needs, but for values and identity. And not only for Ukraine, but for the entire Western world. That is why Ukraine's true victory in the war has global meaning for future humanity. In the current Russian-Ukrainian war, in addition to geopolitical and economic issues, an existential political question is also being decided: who is the authentic descendant of the Kyivan Rus' - Ukraine or Russia? One of the reasons for Russia's war against Ukraine is its existential longing to connect with its historical roots - Kyiv, as "the mother of Rus' cities." This pursuit shapes the war against Ukraine's beyond-rational and existential character. This argument implies that Russia, contrary to its statements, fights primarily not against the collective West or NATO, but settles its age-old dispute with Ukraine with all military brutality. Thanks to the nation's extraordinary resistance, courage, and heroism, Ukraine has literally been etched into the mental map of many people around the world - people who, before Russia's all-out aggression, had no idea where Ukraine was on a world map. That is why it is important today to spread knowledge about Ukraine abroad, promote Ukrainian cultural products, and provide institutional guarantees for this process.

Seventh, the war in Ukraine has become a catalyst for a renewed form of humanism, generating global reverberations, countering neo-totalitarianism, and contributing to the emergence of a new type of civilization. This emerging civilization seeks to overcome war as a means of resolving conflicts among peoples, countries, states, and alliances. Achieving this objective requires exposing and stopping neo-totalitarianism as a fundamentally destructive force for humanity - one

that rejects democracy, human rights, and, ultimately, development [28].

According to experts, the following events are most likely to occur during the 21st century [29]:

1. The formation of a global coalition of democratic states. While facing the threat of Hitler's enslavement of the world, U.S. President Franklin Roosevelt and British Prime Minister Winston Churchill signed the Atlantic Charter on 14 August 1941, which became the basis for the formation of an anti-Hitler coalition of states and ensured the defeat of the Third Reich and its allies. Eighty years later, on 10 June 2021, U.S. President Joe Biden and British Prime Minister Boris Johnson signed a new Atlantic Charter, which proclaims the struggle of democratic countries against the authoritarian regimes of the 21st century. Given their global ambitions, such regimes pose a real threat to humanity and must be minimized as much as possible. Upon the new Atlantic Charter, amid the escalation of the Russian-Ukrainian war, the Ramstein group was formed on 22 April 2022. Ramstein emerged as a series of diplomatic meetings of defense ministers from democratic countries, held to synchronize efforts to accelerate the provision of weapons to Ukraine to counter Russia's large-scale invasion, and to discuss support for Ukraine after the end of the war. It is most likely that Ramstein is a situational democratic alliance for the period of the Russian-Ukrainian war, which, in the post-war period, given the experience of the G7, the North Atlantic Treaty Organization, the EU, and other organizations and alliances, will be transforming into a global network of democracies capable of a rapid collective response to authoritarian provocations.

2. The formation of a global bloc of authoritarian states. These include China, Russia, North Korea, Iran, Syria, Belarus, Venezuela, and several other countries. China openly claims the leadership position in this bloc, although Beijing traditionally avoids institutional forms of military-political interactions with similarly-minded regimes (some sort of alliances or coalitions). The PRC will welcome economic cooperation between authoritarian countries, complemented by the spiritual and psychological closeness of their leaders. The

strengthening of China's position in Africa has both purely economic and political reasons. On this undemocratic continent, local regimes are being selected to serve as reliable partners for the PRC in the long-term historical perspective. China's intention to prove the civilizational superiority of autocracies over democracies by 2049 (the 100th anniversary of the founding of the PRC), even if it means using military force outside its borders, cannot fail to cause concern. In the case of the PRC, we are witnessing the restoration of the imperial attitude of a truly 'great' country (the world's No. 1 economic power) towards other countries and peoples that do not fit within the parameters of Beijing-style great-power politics.

3. The emergence of a new world bipolarity - fundamentally distinct from that of the second half of the 20th century, which was defined by the axis between the geostrategic West led by the United States and the geostrategic East led by the USSR. As argued in paragraphs 1 and 2, there are sufficient grounds to reject both unipolar and multipolar images of the world order. By the mid-century, a bipolar model of the world order will take a clearly defined shape, with the global West, led by the United States, confronting a global East that incorporates elements of the Global South, led by China.

4. De-imperialization of Russia. As a counterweight to China's large-scale imperial preparations, the Russian imperial complex is expected to collapse. This process should be understood as Moscow's abandonment of claims to global dominance and the exhaustion of the resources (primarily economic) needed to sustain such ambitions. Russia is likely to cede some of the territories it acquired in 1945 (the Kaliningrad region and the Kuril Islands), as well as 1.5 million square kilometers recognized as Russian under the 1858 Aigun Treaty and the 1860 Beijing Treaty. Should these territories indeed be returned, China may advance new territorial claims, with no regard for international law. It is also plausible that a renaissance of state-building could occur in the North Caucasus, driven by the restoration of sovereignty in Chechnya-Ichkeria and the declarations of independence by Ingushetia and Dagestan. In such a scenario, several Volga administrative units, most notably Tatarstan, could follow

suit. In any event, Russia's international influence will decline significantly compared to previous eras.

5. A fundamental renewal of existing international organizations (the UN, the Organization for Security and Cooperation in Europe (OSCE), the Council of Europe (CoE)) or the creation of new ones. Most international 20th-century institutions (especially security-related ones) have proven ineffective amid the significant deterioration of the international situation at the beginning of the 21st century. The UN Security Council and the UN as a whole have been rightly criticized for failing to prevent the spread of COVID-19, the Russian invasion of Ukraine, or the recent militarization of states and international relations in general. We face a situation of critical incompatibility between the old instruments of international cooperation (in particular, those for ensuring international security) and emerging threats and dangers. In response, political leaders advance ideas ranging from the dissolution of the UN to the removal of aggressor states from the organization. Given the inertia of international organizations' transformation processes, democratic state actors have already initiated the creation of new intergovernmental associations capable of expanding beyond economic issues to political ones. Notable examples include the US-EU Trade and Technology Council (TTC), the Quad group of nations (Australia, India, Japan, and the US), the AUKUS group (Australia, the UK, and the US), and the I2-U2 group (India and the US). The rapid pace of their formation suggests a high probability that the international structures of the twentieth century will be gradually replaced by similar associations, more attuned to the present situation and offering fresh approaches to its so-called revitalization.

6. The further expansion of the EU (currently 27 states) and NATO (currently 31 states). In contrast to the previous development, the EU and the North Atlantic Treaty Organization (also political products of the previous century) have proven their viability and even sketched out plans for further expansion. The existence of these stable international structures, whose historical prospects appear promising, makes it possible to predict the West's victory in its

confrontation with Eastern dictatorships across at least several areas: economic and technological, security and political, spiritual and informational. Ukraine, albeit belatedly, has nevertheless expressed its interest in joining these Western associations, significantly strengthening its chances of self-preservation and further development in the conflict-ridden Eastern European environment.

7. Proliferation of weapons of mass destruction. Iran seeks to become the tenth nuclear power. It is likely to succeed in this endeavor, seriously undermining global security. China, as the source of COVID-19, has shown new capabilities for developing and spreading biological weapons. Nuclear threshold states, capable of producing nuclear systems but bound by international law, are ready to support the less-than-ideal formula of securing their own safety through the possession of nuclear weapons. Under such conditions, the acquisition of weapons of mass destruction (primarily nuclear) by terrorist actors in international relations, whose radical goals are no longer seen as detached from reality, becomes a real possibility.

8. The emergence and recognition of new states. The total number of state entities worldwide is currently 194 (including the Vatican), with varying degrees of sovereignty and international influence. Nevertheless, the process of state emergence and international recognition continues. For example, Palestine has been recognized by 139 states, Kosovo by 101, and Taiwan by 14. Other cases, such as Catalonia, Western Sahara, the Turkish Republic of Northern Cyprus, the Pridnestrovian Moldavian Republic, South Ossetia, Abkhazia, and Chechnya, remain at the center of ongoing international debates over recognition and non-recognition. Several quasi-state entities assert claims to statehood. These include Jammu and Kashmir in the disputed territory between India and Pakistan; Wa and Shan regions in Myanmar; Awdalland, Azania, Galmudug, Puntland, Somaliland, and Himan and Heeb in Somalia; Syrian Kurdistan; Cabinda in Angola; Waziristan in Pakistan; Tamil Eelam in Sri Lanka; and the Islamic State (Islamic State of Iraq and the Levant) in Iraq, Syria, and Libya. In Europe, debates have also emerged around the prospect of an independent Scotland, the Basque Country, and Padania. In many

cases, declarations of independence provoke armed intervention by external actors, either supporting or opposing the emergence of a new actor in the international system. Ukraine has directly experienced this through the conflicts involving the self-proclaimed "DPR" and "LPR," as well as the "PMR" within Moldova.

9. The rise of religious extremism, predominantly illegal armed groups of Islamic origin. Recent religious and political history already includes the movements Hezbollah (1982–present), Hamas (1987–present), Al-Qaeda (1988–present), the Taliban (1994–present), Boko Haram (2002–present), and ISIS (Islamic State of Iraq and the Levant) (2014–present). The idea of proclaiming a global caliphate, which would include Podillia, the Northern Black Sea region, and Crimea, among other lands, may be viewed negatively by European countries. However, it will also have many supporters, especially among newly formed Islamist movements, whose numbers are not decreasing.

10. Restoration of Ukraine's territory within the internationally recognized state borders of 1991. The weakening of Russian statehood will have many consequences, including the restoration of Ukraine's territorial integrity and, consequently, its political strengthening. In the longer term, further integration between Ukraine and Poland may be expected, with both states emerging as key actors in Eastern Europe. Such cooperation could function as a "democratic safeguard" against Russian revanchism, potentially on the basis of a new security and defense alliance linking the Baltic and Black Sea regions.

It is important to note that leaders of democratic states (given the anticipated success of upcoming elections) often display excessive caution in situations that require political assertiveness. This tendency is reflected in their reluctance to adopt decisions that, in the view of Western ruling elites, might alienate voters, as well as in their unwillingness to narrow the conventional "comfort zone" that has become an integral feature of Western societies in the post–World War II era. Most Western European citizens avoid contemplating the possibility of war on their own territory or personal involvement in

combat operations. Modern democracies must evolve, particularly by fostering public readiness to resist authoritarian influences on rights, freedoms, and human dignity. Such readiness should become an integral component of political thought and civic culture. At present, however, it is often overshadowed by unfounded indulgence, unjustified tolerance, and an inexplicable patience toward anti-human and anti-democratic impulses promoted by authoritarian forces targeting the Western world.

Considering the numerical dominance of democratic states over autocratic ones in the international system, the global community has the potential to first contain, and then dismantle, the global "axis of evil." However, these efforts have only just begun. For these processes to succeed, they require a renewed commitment to democratic socialization among citizens and their active participation in democracy.

Experts from the Ukrainian Center for Economic and Political Studies (the Razumkov Center), well-regarded in Ukraine and internationally, provide alternative geopolitical insights that align with this view. They suggest the following elements should be included in the global geopolitical transformations [30].

First, two civilizational groups - democratic and autocratic - are establishing themselves on a strategic level. The vast majority of countries face a choice between two sets of strategic development guidelines and the underlying core values. Simultaneously, countries are determining the acceptable level of compromise between their proclaimed values and the economic benefits required to sustain everyday living conditions. The countries' response to the Russian-Ukrainian war launched in 2014 is a compelling illustration of these processes. Among the key indicators of alignment with either Russia or Ukraine in this civilizational conflict is the support or non-support for international sanctions against Russia, the decision to supply or not to supply Ukraine with weapons and military equipment, and the willingness or unwillingness to "press" Russia to the point of defeat, which would mean the reformation of the Russian political leadership and the transition of the Russian political system to a non-authoritarian basis.

Second, amid Russia's full-scale aggression against Ukraine, closely monitored inside and outside Europe, states are rethinking state-building strategies. It is becoming evident that a country's socioeconomic base, taken in isolation, is highly vulnerable to external aggression. Accordingly, a priority for the majority of states is to update (in fact, re-establish) the security and defense base for state development, capable of protecting key areas of society, including politics, economics, and information, through a modernized security and defense sector. The institution of strategic partnership of the state and its entry (or non-entry) into international security structures is of paramount importance in these circumstances.

The third trend from the Razumkov Center: the lessons of the Russian-Ukrainian war suggest a narrowing of Russia's geopolitical project, initially aimed at subjugating countries and peoples not only in the post-Soviet space but also beyond it (i.e., the former socialist states of Central and Eastern Europe, as well as former socialist-oriented countries). Ukraine's struggle for freedom and independence has triggered an irreversible shift in many countries' understanding of new development priorities grounded in democratic values. Russia's imperial potential is deteriorating. This further confirms the unfounded nature of Russia's geopolitical claims to former "historic" territories and ideological allies. Objectively, this creates the conditions for the collapse of the "last empire," amid growing centrifugal tendencies in its internal dynamics.

Therefore, we observe a wide range of scientific approaches to the main geopolitical trends of the 21st century. There are clear differences between the polar approaches adopted by China (in its interactions with Russia and other autocracies) and the U.S. (in its close communication with its democratic allies) regarding strategic issues of world order and the building of a new international relations system. Human rights and freedoms-based democratic societies (of which Ukraine is a member) oppose autocratic societies where power is elevated to absolute and political extremes, including nuclear war, prepared for the sake of illusory world dominance.

The confrontation between democracies and autocracies is likely to intensify in the short term. The risk of an armed conflict extending beyond the Russian-Ukrainian war, involving new actors and a broader array of weapons, appears quite feasible. Such a confrontation could lead to the creation of a new international system, markedly different from the frameworks of the 20th century—such as Versailles, Yalta-Potsdam, and Belovezhskaya. Achieving this would require the democratic side of humanity to overcome its authoritarian opponent. While Ukraine is involved in these developments, its influence remains limited, preventing it from matching the major global geopolitical powers.

Overall, the following patterns in the formation of a new security environment could be identified:

- The new world order is being shaped by two real centers of power (the U.S. and China), which have the potential for both constructive and destructive interaction;
- **Nuclear terrorism, weapons control, disarmament, climate change, and artificial intelligence (AI) are becoming key topics on the international agenda;**
- A sharp increase in military spending is expected in the near future;
- **Transatlantic security will be closely tied to the situation in the Indo-Pacific region, around Taiwan, and on the Korean Peninsula. A steady trend is toward the formation of a system of small security alliances rather than a global NATO-like structure in Asia.**
- **Amid the ongoing confrontation between the US and China and Russia's aggression against Ukraine, relations with middle powers (countries of the so-called Global South) will be a major factor in the evolution of geopolitical and geoeconomic situations.**
- **The prospect of creating economic blocs in which democratic countries seek to curb the supply of "sensitive materials" from autocratic countries and limit their ability to develop dual-use technologies is becoming increasingly relevant.**

Conclusions to Section I

Military power is gradually replacing civilizational and international-legal factors, emerging as the dominant force in the new global order.

New realities in international relations necessitate addressing international security challenges at the global and regional levels. The effectiveness of international security institutions will largely depend on the mechanisms for applying coercive measures. Accordingly, a new paradigm for shaping the international security environment must rest on recognition of the unity of the world and the indivisibility of security, as well as the capacity to counter emerging threats.

Moreover, today's security landscape carries the risk of direct military conflict between major powers. China's territorial claims challenge U.S. allies from Japan to the Philippines and other U.S. partners in regions such as India and Vietnam. Long-standing U.S. interests, such as freedom of navigation, are coming into direct conflict with China's maritime ambitions.

A series of coups across Africa since 2020 has allowed Moscow to strengthen its position on the continent, despite directing massive military and economic resources toward the war in Ukraine. The increasing military, political, and economic influence of Russia in several countries, now including Burkina Faso, the Central African Republic, Mali, and Sudan, runs counter to the expectations expressed by U.S. Secretary of State Antony Blinken. In June 2023, he stated that the full-scale invasion of Ukraine had "reduced Russia's influence on all continents." More than two years after the outbreak of this war, Russia clearly remains capable of expanding its influence in Africa and other parts of the world.

Given the demographic makeup of many countries in the Global South, especially the large proportion of young people, it is wise to create a dedicated public diplomacy effort. This initiative should focus on increasing support for Ukraine by explaining the causes of the war, the current situation, and by identifying topics that resonate with younger audiences. With elections approaching in many significant

countries, this factor may influence the politicians that young people support in their respective nations.

Ukraine should actively leverage the opportunities and platforms of various international organizations, including those that represent Global South countries, in addition to the United Nations. Alongside the Association of Southeast Asian Nations (ASEAN) and the African Union, where Ukraine has recently increased its engagement, it is essential to maintain ongoing communication with other bodies. These include the Economic Community of West African States (ECOWAS), the Asia-Pacific Economic Cooperation (APEC), the Organization of American States (OAS), and the League of Arab States. Additionally, parliamentary diplomacy will play a significant role for many countries in these regions. Therefore, Ukraine should make better use of the resources provided by the Inter-Parliamentary Union, where Ukrainian lawmakers have increased their engagement.

We can confidently state that the world, along with the system of international relations, is undergoing a significant transformation. The nature of this change has become virtually impossible to analyze using previous approaches. In current context, it is essential to take into account a complex array of factors influencing international actors, including situational alliances, civil society, non-governmental initiatives, sovereign nations, and associations of states. In light of this, conclusions and recommendations addressed to state authorities by information-analytical institutions must be reliably verified, repeatedly cross-checked, and should in no case claim long-term applicability.

References:

1. Panfilov, O. Y., & Petrova, L. O. (2020). Faktor voiennoi syly v suchasnykh mizhnarodnykh vidnosynakh [The factor of military force in modern international relations]. *Visnyk Natsionalnoho universytetu "Iurydychna akademiia Ukrainy imeni Yaroslava Mudroho", Seriia: Filosofiia, filosofiia prava, politolohiia, sotsiolohiia*, 4(47), 113–126. https://doi.org/10.21564/2075-7190.47.218965

2. Bodruk, O. S. (2002). Faktor syly v suchasnomu sviti [Power factor in the modern world]. *Polityka i chas*, (3), 57–67.

3. Bodruk, O. (2005). Sylova hran bezpeky [The power frontier of security]. *Polityka i chas*, (4), 47–56.

4. Orlyk, V., & Hrytsenko, A. (2022, October 14). *Osnovni polozhennia novoi Stratehii natsionalnoi bezpeky SShA* [The main provisions of the new US National Security Strategy]. https://niss.gov.ua/doslidzhennya/mizhnarodni-vidnosyny/osnovni-polozhennya-novoyi-stratehiyinatsionalnoyi-bezpeky (Accessed April 25, 2025)

5. Bielieskov, M. (2022, December 14). *Natsionalna oboronna stratehiia SShA 2022 roku: osnovni polozhennia, otsinky i naslidky dlia Ukrainy* [US National Defense Strategy 2022: main provisions, assessments, and consequences for Ukraine]. https://niss.gov.ua/doslidzhennya/natsionalna-bezpeka/natsionalna-oboronnastratehiya-ssha-2022-roku-osnovni (Accessed April 15, 2025)

6. Honchar, M. (2023). *Bezpekovi vakuumy yak naslidok viiny Rosii proty Ukrainy: otsinka vplyvu i mozhlyvi shliakhy podolannia* [Security vacuums as a consequence of Russia's war against Ukraine: impact assessment and possible ways to overcome]. https://geostrategy.org.ua/analityka/analitychna-zapyska/bezpekovi-vakuumyyak-naslidok-viyny-rosiyi-proty-ukrayiny-ocinka-vplyvu-i-mozhlyvishlyahy-podolannya (Accessed April 11, 2025)

7. Razumkov Centre. (2022). *Rol i mistse Ukrainy v perspektyvnykh yevropeiskii ta yevro-atlantychnii systemakh bezpeky* [The role and place of Ukraine in promising European and Euro-Atlantic security systems] (Research Report). https://razumkov.org.ua/images/2022/11/16/2022_Rolj_i_mistce_Ukr.pdf (Accessed January 17, 2025)

8. Zaluzhnyi, V. (Ed.). (2023). *Rik viiny za svobodu: Voienno-istorychnyi narys rosiisko-ukrainskoi viiny (24.02.2022-24.02.2023). U 4-kh kn. Kn. III* [A year of war for freedom: A military-historical essay of the Russian-Ukrainian war (24.02.2022-24.02.2023). In 4 books. Book III]. Kyiv, Ukraine: Vydavnytstvo Lira-K.

9. Solohub, I., & Fedyk, A. (2023, December 4). Naklasty lapu na krytychno vazhlyvi resursy Afryky: u shcho investuiut Kytai ta Rosiia [Laying hands on Africa's critical resources: what China and Russia are investing in]. *Ekonomichna Pravda*. https://www.epravda.com.ua/publications/2023/12/4/707291/ (Accessed April 15, 2025)

10. Siegle, J. (2021). Russia and Africa: Expanding influence and instability. In G. P. Herd (Ed.), *Russia's global reach: A security and statecraft assessment* (pp. 80–90). George C. Marshall European Center for Security Studies. https://www.marshallcenter.org/en/publications/marshall-center-books/russias-global-reach-security-and-statecraft-assessment/chapter-10-russia-and-africa-expanding-influence-and (Accessed April 15, 2025)

11. Tiflisli, N. (2024, April 20). Afro-Rosiiska imperiia. Navishcho Moskvi Sakhel? [Afro-Russian Empire. Why does Moscow need the Sahel?]. *TRT Russian*. https://www.trtrussian.com/mnenie/afro-rossijskayaimperiya-zachem-moskve-sahel-17840160 (Accessed April 15, 2025)

12. Siegle, J. (2023, January 6). Decoding Russia's economic engagements in Africa. *Africa Center for Strategic Studies*. https://africacenter.org/spotlight/decoding-russia-economic-engagements-africa/ (Accessed April 15, 2025)

13. Congressional Commission on the Strategic Posture of the United States. (2025). *The Final Report of the Congressional Commission on the Strategic Posture of the United States*. https://www.ida.org/-/media/feature/publications/A/Am/Americas%20Strategic%20Posture/Strategic-Posture-Commission-Report.pdf (Accessed June 25, 2025)

14. U.S. Department of Defense. (2025). *Statement on the Development of the 2025 National Defense Strategy*. https://www.defense.gov/News/Releases/Release/article/4172735/statement-on-the-development-of-the-2025-nationaldefense-strategy/ (Accessed May 25, 2025)

15. Korsunskyi, S. (2024, August 13). Yak Ukraini zavoiuvaty umy Azii [How Ukraine can win the minds of Asia]. *Dzerkalo Tyzhnia*. https://zn.ua/ukr/WORLD/jak-ukrajini-zavojuvati-umi-aziji.html (Accessed July 15, 2024)

16. UN General Assembly. (2024). *Aggression against Ukraine: resolution / adopted by the General Assembly*. https://digitallibrary.un.org/record/3965290?ln=ru&v=pdf (Accessed July 16, 2024)

17. Comfort, E. (2024, April 1). The trouble with "the Global South." *Foreign Affairs*. https://www.foreignaffairs.com/world/trouble-global-south (Accessed July 25, 2024)

18. Miliband, D. (2024, April 18). The world beyond Ukraine: The survival of the West and the demands of the rest. *Foreign Affairs*. https://www.foreignaffairs.com/ukraine/world-beyond-ukraine-russia-west Accessed July 25, 2024)

19. Horodyskyi, A. (2024, March 14). Shcho take Hlobalnyi Pivden, choho vin khoche i chomu pro noho stilky hovoriat? [What is the Global South, what does it want, and why is it talked about so much?]. *RFI*. https://www.rfi.fr/uk/міжнародні-новини/20230314-що-таке-глобальний-південь-чого-він-хоче-і-чому-про-нього-стільки-говорять (Accessed July 15, 2024)

20. Henley & Partners. (2024). *The Africa Wealth Report 2024*. https://www.henleyglobal.com/publications/africa-wealth-report-2024 (Accessed July 16, 2024)

21. Oxfam. (2024). *The Middle East and North Africa Gap*. https://oxfamilibrary.openrepository.com/bitstream/handle/10546/621549/bp-mena-gap-prosperity-for-the-rich-austerity-for-the-rest-051023-en.pdf (Accessed July 17, 2024)

22. BBC News Ukrainian. (2024). *Zirky, polityky i mahnaty pryikhaly z usoho svitu na rozkishne vesillia v Indii* [Stars, politicians, and tycoons came from all over the world for a luxury wedding in India]. https://www.bbc.com/ukrainian/articles/crgevp9d1v9o (Accessed July 17, 2024)

23. Pagel, H., Ranke, K., Hempel, F., & Köhler, J. (2014, July 11). *The use of the concept "Global South" in Social Science & Humanities* [Conference presentation]. Globaler Süden / Global South: Kritische Perspektiven, Humboldt-Universität zu Berlin, Berlin, Germany. https://www.academia.edu/7917466 (Accessed July 25, 2024)

24. Bordilovska, O. (2024). *Hlobalnyi Pivden u konteksti novykh vyklykiv* [The Global South in the context of new challenges]. https://

niss.gov.ua/doslidzhennya/mizhnarodni-vidnosyny/hlobalnyy-pivden-u-konteksti-novykh-vyklykiv (Accessed June 25, 2024)

25. McMaster, H. R. (2023). *Polia bytvy. Borotba za zakhyst vilnoho svitu* [Battlegrounds: The Fight to Defend the Free World] (N. Koval, Trans.). Kyiv, Ukraine: Nash Format. (Original work published 2020)

26. Smolii, V. A., & Yas, O. V. (2022). Suchasna rosiisko-ukrainska viina u svitli postkolonializmu [Modern Russian-Ukrainian war in the light of postcolonialism]. *Visnyk NAN Ukrainy*, 6(36), 3–16.

27. Kozlovets, M. A. (2023). Svitovyi poriadok XXI stolittia: vektory transformatsii [World order of the 21st century: vectors of transformation]. In *Proceedings of the XXXV Kharkiv Political Science Readings* (pp. 20–25). Kharkiv, Ukraine: Pravo.

28. Pyrozhkov, S. I., & Khamitov, N. V. (2022). Viina i myr v Ukraini: shliakhy do realnoi peremohy i rozvytku [War and peace in Ukraine: paths to real victory and development]. *Visnyk NAN Ukrainy*, 9(39), 38–49.

29. Smolianyuk, V. F., & Hunin, V. Ye. (2023). Svitovyi poriadok XXI stolittia: vektory transformatsii [World order of the 21st century: vectors of transformation]. In *Proceedings of the XXXV Kharkiv Political Science Readings* (pp. 40–44). Kharkiv, Ukraine: Pravo.

30. Razumkov Centre. (2022). *Heopolitychni ta heoekonomichni zminy, formovani pid vplyvom rosiiskoi ahresii, ta onovlennia mistsia Ukrainy u svitovomu prostori* [Geopolitical and geoeconomic changes shaped by Russian aggression and renewal of the place of Ukraine in the world] (Research Report). Razumkov Centre.

SECTION II

THE NEW GENERATION OF RUSSIAN WARS: MAJOR TRENDS AND CONCEPTS

2.1. Emerging Trends in Modern Warfare Capabilities

The war between the Russian Federation and Ukraine has been going on for more than ten years. Today, it has been the longest war, the longest violent conflict in Europe since the Second World War.

Times of war encourage us to reflect on their essence, because it is precisely at turning points that we have the opportunity to directly feel and understand the obvious and hidden meanings of events. Recently, numerous researchers and experts have noted that the strategic interests of modern states have not disappeared but, on the contrary, have intensified. Accordingly, modern military conflicts have acquired new characteristics compared to the past, when the focus was on military dominance.

When studying trends in the development of military struggle in modern conditions, it would be advisable first to conduct a retrospective analysis of the evolution of the theory of the generations of modern warfare (Global Modern Wars, GMW).

In the 1980s, American researchers introduced the concept of four generations of warfare into scientific and military discourse.

William S. Lind and his co-authors first presented the GMW theory in their 1989 article published in the Marine Corps Gazette. In this article, they suggested that the history of modern warfare from the Treaty of Westphalia in 1648 to the present can be viewed as a history of four generations of warfare [1].

The first generation (1GW) refers to the wars of the early modern period and the beginning of the industrial era (from the mid-17th to the first half of the 19th century), which were characterized by the use of linear tactics, the creation of professional national armies, and

were associated with the very emergence of the modern concept of war as a war between states, which was formed around the ideas of Carl von Clausewitz. 1GW relied primarily on human strength.

The emergence of the second generation of modern warfare (2GW) was linked to the development of new forms of transport and communication, primarily railways, and of new and improved firearms and artillery (especially indirect artillery and machine guns). The central aspect that distinguished the second generation of wars, the most important example of which was the First World War, was its focus on achieving technological and numerical superiority in weapons and mobilized troops, with the aim of dominating the front lines with firepower to exhaust the enemy.

This approach gradually led to the emergence of the concept of 'total war,' which was introduced by one of the outstanding commanders of the First World War, General Erich Ludendorff. Unlike first-generation wars, which strictly separated the military from the civilian population, the concept of 'total war' proposed general conscription and the mass involvement of civilians in the war effort.

Third-generation wars (3GW), the most striking examples of which are World War II and blitzkrieg tactics, are characterized by the search for new ways to achieve victory in 'total war' that leverage the advantages of strategic thinking. Accordingly, the basis of the third-generation warfare is mobility and maneuverability.

Unlike the previous three generations of warfare described in Lind's article, which were based on historical examples, the identification of the fourth generation was more related to the prospects of military futurology. At the time Lind wrote the article, the U.S. Army and Marine Corps were only 'trying to cope with the changes of the third-generation warfare.' In this light, Lind and his co-authors attempted to predict the uncertain future of warfare using the concept of fourth-generation warfare. Initially, the article's description of the future of warfare included aspects of technological and social change.

From the perspective of Dr. Robert J. Banker (1996), who later compared Lind's ideas with those of other military strategists of the time, attitudes towards the future of war after the end of the Cold War

were broadly divided into two main approaches, the first one being more technology-oriented, while the second was "humanitarian" and emphasized the role of ideas and social factors. The first approach was largely associated with the ideas of Alvin and Heidi Toffler, who proposed the concept of third-wave warfare, which assessed the advantages of high-tech warfare, which, in turn, secured military superiority for post-industrial countries. One part of Lind's fourth-generation warfare concept, as described in his 1989 article, was technology-oriented because, similarly to the Tofflers' approach, it also envisaged the development of high-tech military weapons, such as directed energy weapons and robotics, while the other part was more 'humanitarian' and envisaged the growth of types of warfare known as 'asymmetric,' including the growth of terrorism.

[Martin van] Creveld focused on Carl von Clausewitz's ideas as the ones that shaped the modern meaning of war. He described this meaning as 'trinitarian,' that is, a meaning based on Clausewitz's trinitarian view of war, which posited three basic elements: 'government,' 'army,' and 'people.' Creveld argues that the new type of warfare now gaining momentum is becoming 'non-trinitarian,' undermining Clausewitz's long-standing view of wars as being waged by governments using their armies and supported by their people. Instead, the new generation of wars is blurring the lines between combatants and civilians and bringing in new players, like ethnic, social, and religious movements, criminals, and transnational business groups, while governments are slowly losing their monopoly on war. Therefore, everything in military history seems to be returning to the conditions that existed before the 1648 Treaty of Westphalia, which created the preconditions for the modern image of war. At the same time, these changes are also linked to the creation of so-called low-intensity conflicts, which, in turn, stem from the impossibility of waging full-scale 'total war' in the nuclear age and, despite their name, are often characterized by particular cruelty and bloodshed. On the other hand, these changes were represented by the growth of phenomena such as revolutionary movements, national liberation movements, religious movements, and anti-colonial struggles, which

initiated and won asymmetric wars against significantly more powerful enemies, for example, the war in Algeria, the war in Vietnam, the war in Afghanistan from 1979 to 1989, and others. In such wars, these movements introduced completely new (from the point of view of modern warfare) principles that led to the mass involvement of the population in the struggle, the blurring of the lines between combatants and non-combatants, effective guerrilla warfare, the demoralization of the enemy (including within the enemy's own country), and the manipulation of world public opinion regarding the events.

Thus, 4GW is not a new idea, as in this context it emerged as a widespread phenomenon in the historical context of the collapse of the colonial system after the end of the Second World War and was very often associated with positive changes in socio-political life and the struggle of various categories of people for their freedom, which undermined the old structures of power and oppression. However, in recent decades, this way of waging war has also become closely linked to the rise of international terrorism, which uses methods that can never be justified and has now become a universally recognized global threat. In this context, Creveld (1991) asserts that modern states are ill-equipped to confront the challenges posed by fourth-generation warfare (4GW) due to their lack of understanding of new methods of warfare.

Some researchers, in connection with radical changes in the means of military struggle, distinguish six generations of military conflicts that have successively replaced one another. In the first generation of warfare, the primary weapons were cold steel, and the main goal was to destroy the enemy and seize their weapons and valuables. In the second generation, war was characterized by the destruction of the enemy, the seizure of their territory and valuables, and the primary weapon was a smoothbore. In third-generation warfare, the destruction of the enemy's armed forces, their economy, and the seizure of territory are characteristic. The primary type of weapon in this generation is rifled multi-shot weapons with increased rate of fire, accuracy, and range. Automatic and rocket weapons, mechanized troops, tanks, aircraft, aircraft carriers, and submarines are

replacing third-generation weapons. The main goal of fourth-generation warfare is to destroy the enemy's armed forces, ruin its economic potential, and overthrow its political system. Fifth-generation warfare involves nuclear weapons, which do not achieve their targets but pose a threat to the destruction of civilization or entire continents. Sixth-generation warfare is aimed at undermining the economy, management systems, and vital functions of the state, as well as destroying military facilities. The main types of weapons in this war are high-precision weapons (HPW), weapons based on new physical principles (NPP), information weapons, and electronic warfare forces and means.

In other words, the phenomenon of war is constantly evolving as the world changes. This must be taken into account when considering future trends in armed conflict. What are the main trends in armed conflict that we can identify for the future?

Y. Kobets suggests distinguishing among seven types of probable 21st-century wars. These wars differ significantly from one another in many respects, including the criterion of effectiveness [2].

The general list of wars includes:

- Classical technogenic-force war.
- Economic war.
- Undeclared genocide against the population of a rival state.
- Organizational war (cases of introducing external or hostile organizational structures into the national state system of the opposing side, for example, illegitimate authorities or various foundations).
- Information warfare.
- Chronological warfare – a method of waging war through the deliberate reinterpretation of a country's 'unpleasant' past and the constant manipulation of historical facts in favor of the customer.
- Spiritual warfare, another method of waging war that involves imposing dangerous values on subjugated peoples or states. This method aims to change the spiritual principles and values of these peoples or states to achieve its goals. In turn, M. Trebin and T. Chernyshova propose the following trends in future armed conflict [3]:

First, a retrospective look at the evolution of military art shows that its development trajectory represents the mastery of space in which an ever-expanding armed conflict is being waged. This expansion took place from the strategy of a general battle at a single point (the era of the Napoleonic Wars) to a linear strategy (from the second half of the 19th century till the mid-1930s), and then to deep operations in the continental theatre of war (CTW) (World War II) and large-scale (air-space, air-ground and land-sea) operations at the beginning of the 21st century. In other words, traditional military actions, strictly divided by physical domains, have been replaced by comprehensive actions conducted simultaneously across all domains of confrontation in a significantly expanded space-time continuum. This introduces the multi-domain principle, to be further developed in the future.

Second, the increasing spatial indicators of armed conflict, the growing significance of the information continuum must be acknowledged. At the current stage of civilization, information is central to the functioning of social and state institutions and in the life of every individual. Informatization creates a single global information space, facilitating the production, accumulation, processing, storage, and exchange of information among individuals, organizations, and state entities. The rapid exchange of political, economic, spiritual, scientific, and technical information, along with the adoption of new information technologies across all sectors of public life, particularly in production and management, offers clear advantages. However, as industrial growth has threatened Earth's ecology and advances in nuclear physics have posed the danger of nuclear war, informatization may also pose a broad spectrum of challenges.

Information weapons primarily target two domains. The first is anthropogenic, encompassing humans, their intellect, and society's collective consciousness. The realities of contemporary being indicate that direct influence on individuals can effectively achieve the objectives of information warfare. Studies from the late twentieth century report that mental disorders occur in 4–6% of military personnel during routine activities, 15–20% during training and combat

activities, and 30–86% during active combat, depending on factors such as intensity and casualty rates. The second domain is technogenic, which includes software and information support, hardware, telecommunications equipment, communication channels, and integrated control systems. The most vulnerable components of this infrastructure are telecommunications nodes, satellite communication centers, and international information exchange channels.

Third, the growing importance of outer space. According to American experts, the main tasks of combat space assets during military operations from space are aimed at inflicting losses on the enemy across continental, oceanic, and maritime theaters of operations, and in airspace. These tasks involve destroying ground-based space forces and assets, such as elements of launch and control areas and information processing facilities. They also aim to destroy stationary and mobile strategic nuclear forces, including launchers and control centers. Combat space assets also target mobile groups of surface ships and submarines.

Additionally, they focus on strategic aviation aircraft at airfields and in airspace, as well as on important strategic facilities, and on manpower, weapons, and military equipment. Other goals include creating active jamming of radio-electronic means and having a global impact on the natural environment of the enemy's territory. Military analysts also believe that space assets can be used for tasks such as global and local control from space over the status and dynamics of troop or naval groupings in any region of the world. Further uses include information, coordinate-metric, and other types of support for their actions, and the management of them from a single center located at any distance from the region of combat, operational, or strategic actions. This management supports greater independence in decision-making by all levels of military command.

Fourth, the expansion of the range of means of warfare. The importance of the New Physical Principles Weapons (NPPW), as well as high-precision, hypersonic, and cyber weapons; information and control equipment; military robotic vehicles (RCV); crewless aerial and autonomous marine vehicles; and the use of AI in decision-mak-

ing support systems, troop (force) and weapons management, and military and special equipment.

The focus of military operations in future wars is expected to be on weapons that operate on the new physical principles. The use of NPP weapons involves the momentary defeat of the enemy at a great distance by delivering directed energy. These may include laser weapons that deliver gamma, X-ray, ultraviolet, visible, or infrared electromagnetic radiation to the target; radio frequency weapons – delivery of electromagnetic radiation energy within the radio frequency wavelength range (ultra-high frequency weapons, infrasound weapons, etc.); beam (accelerator) weapons – the delivery of directed beams of high-energy charged or neutral particles accelerated to nearly the speed of light to the target. All such weapons deliver striking energy to the target almost instantaneously, with a range of many hundreds of kilometers. The implementation of this principle of targeting hostile objects could radically change the nature of war in the future. The use of such weapons will enable the destruction of targets without physically destroying them, reduce the need for conventional means of armed combat, and shorten the duration of operations to minutes. With zero-limited killing, such weapons can disrupt the operation of phones, radars, computers, and other means of communication, as well as guidance, navigation, and control. Plans are also in place to employ "combustion-inhibiting" agents that stop vehicle engines, as well as chemicals that destroy car and aircraft tires when sprayed on roads and airfields. The emphasis is on using such means to disable troops without destroying them.

In the late 20th and early 21st centuries, the experience of fighting in urban areas (in city settings) gathered by many countries' armed forces in local wars and military conflicts led to the development of a new type of weapon: the MRV. Main tasks assigned to MRVs include: fire support for advancing units, guidance of high-precision strike systems, terrain reconnaissance and monitoring of enemy target destruction outcomes, recon and surveillance, delivery of ammunition, fuel, and supplies to combat zones, etc.

In future wars, the nature of air combat operations will change dramatically due to the wider use of MRV systems such as unmanned aerial vehicles (UAVs) and stealth devices. With the widespread use of UAVs, plans call for expanding the combat capabilities of ground forces and reconnaissance and sabotage units. UAVs will be used both as individual systems and as unmanned aviation formations. Depending on flight range, combat load, and assigned missions, UAVs will be used at various levels, from tactical to strategic. The flight duration, as evidenced by experimental flights of U.S. UAVs, can be measured in years. Applications of unmanned aviation can include reconnaissance and strike operations, airspace control, etc.

The use of AI technologies in new weapons-control systems will enable breakthroughs in combat operations. Such systems will accelerate decision-making by accounting for the maximum number of factors, significantly reduce the cycle of troop (force) control, and increase combat capabilities. To date, American specialists have achieved the greatest results in the field of "deep machine learning." This has been made possible by rapid progress in the development of multi-level artificial neural networks. Image recognition and machine learning technologies used in modern AI can enable high levels of automation in management decision-making by analyzing and processing information from various sources.

Fifth, a shift in the logical and temporal structure of armed combat: gaining initiative and advantage in the information sphere (in the management of troops and weapons); creating an advantage in the air and space sphere; changing the balance of power on land and sea in one's favor; achieving overall quantitative and qualitative superiority in forces and means; increasing the duration of preparatory actions and reducing the period of active operations; strengthening deductive and weakening inductive links and relationships in armed combat; using strategic and operational means to defeat the tactical link; organizing and conducting armed combat in real time; transition from commanding troops to commanding armed combat.

The current war in Ukraine is a completely new phenomenon in military history. Sean McFate points out that the Russian-Ukrainian

war showed not only how the rules of war have changed, but also how to fight and beat stronger armies in the 21st century. He came up with ten rules [4]:

Rule 1. Conventional war is a thing of the past.

A "conventional war" is one type of combat operation – World War II is an example of this; however, there is currently nothing more unconventional than conventional war. Since 1945, only 6% of wars have been conventional, and the last one was fought 40 years ago. No one fights like that anymore because it no longer leads to victory – but Russia tried. In February 2022, it launched its first conventional war in 35 years and was defeated. A symbol of its strategic incompetence was the 64-kilometer-long Russian military convoy that got stuck en route to Kyiv in the first weeks of the war. Conducting a conventional war requires an extraordinary level of discipline, management, and organizational unity, which the Russians lack. The war was doomed to failure, and the Russians finally changed their tactics at the end of March, switching to the Russian unconventional warfare we saw in Grozny and Aleppo. This is a strategy of terror. This rule explains why traditional wars fail today and suggests what works better.

Rule 2. Invest in people, not technology.

Many imagine future warfare to be extremely high-tech. Yet, the combat experience of technologically advanced armed forces since 1945 has been pathetic, with these forces regularly losing to low-tech armies. France was defeated in Algeria and Indo-China, Britain in Palestine and Cyprus, the USSR in Afghanistan, the U.S. in Vietnam, Somalia, Iraq, and Afghanistan, and Russia, now in Ukraine. The images of a humble Ukrainian tractor hauling Russian tanks off the battlefield say it all. This rule explains why the best technology is the 15 centimeters between our ears. Cunning triumphs over high-tech brute force.

Rule 3. There is no war or peace – they always coexist.

Clever opponents take advantage of the space between war and peace to achieve victory. In 2014, Russia used "little green men," special forces units, and mercenaries such as the Wagner Group to carry out a covert occupation in eastern Ukraine. Ukrainians were not fooled,

unlike the West. For the West, it did not look like a conventional war, but it was not a state of peace either. While Western intelligence agencies were still trying to figure out what Russia was doing in Donbas, the annexation of Crimea became a fait accompli. This rule explains why there is no such thing as war or peace, but only war and peace. The strategy for victory depends on understanding the difference.

Rule 4. Hearts and minds do not matter.

Winning the hearts and minds of the local population does not lead to victory, as most American generals in Afghanistan and Iraq mistakenly believed. And that is one of the reasons for their defeat. During the Vietnam War, there was a saying among U.S. Army special forces soldiers: "If you've got them by the balls, their hearts and minds will follow. " Such is the Russian approach to fighting insurgents, and it involves mass killings of civilians and the obliteration of cities. This is exactly what they did in Chechnya, Syria, and now Ukraine. Human rights violations and associated losses are not a mistake but a hallmark of Russian warfare, as evidenced by Bucha, Mariupol, and Izium. It is an immoral and despicable approach that has been used throughout history, often successfully. This rule explains why violence is usually more effective than mercy in war.

Rule 5. The best weapons do not fire bullets.

"The fight is here. I need ammunition, not a ride." That was one of the most quoted lines said during the Russian invasion of Ukraine, the words of the daring Ukrainian President, who refused the U.S. offer to leave Kyiv. It doesn't matter if this quote is real or not. It had an effect. Weapons began to arrive, and NATO took action for the first time in 30 years. Ukraine successfully turned social media and memes into weapons, easily bypassing the world champion of disinformation – Russia. Rule 4 tells us that hearts and minds are immaterial at the lower, or "tactical," level of warfare. But at the global, or "strategic," level, winning hearts and minds is a prerequisite for victory. The Ukrainian people and government are waging a successful information war that has turned Russia into a pariah state that even China is shunning. More importantly, this has kept the West interested in Ukraine, leading to an increase in weapons, ammuni-

tion, valuable intelligence, diplomatic and popular support. This rule explains why, in the information age, information is more powerful than lethal weapons, and how to use it effectively.

Rule 6. Mercenaries are back in the game.

Russian mercenaries, such as the Wagner Group, became synonymous with war. Since 2014, the Wagner Group has become Putin's favorite weapon because it allows the Kremlin to plausibly deny its involvement in the event of failed operations, and the Russians do fail. In 2018, the Wagner Group clashed with U.S. Special Operations Forces in eastern Syria and was destroyed. Both Moscow and Washington decided to ignore this incident to avoid provoking World War III, which would have been a real possibility if Russian soldiers had been involved rather than military mercenaries. Mercenaries - the second oldest occupation - are a major problem in war. This rule explains what these problems are, how mercenaries are reshaping war, and how best to use or defeat them.

Rule 7. New types of world powers will rule.

This rule does not apply to Ukraine to the same extent as it does to other armed conflicts across the world, such as the drug wars in Latin America, conflicts in Africa, and religious wars in the Middle East and South Asia. Nation-states everywhere are losing ground and being replaced by a new class of global actors: the ultra-rich. According to the World Bank, of the 100 largest profit generators in the world, 71 are corporations, and only 29 are states. In human terms, the richest 1% own 45% of the world's wealth, while the poorer half of the planet's population collectively owns less than 1%. Now that mercenaries are returning, the super-rich can become armed and very dangerous. They can start wars to protect their international interests, just as states do. One day, ExxonMobil or Elon Musk may have their own armies. In fact, they can already if they want to. This rule explains how this will fundamentally change the world order.

Rule 8. There will be wars without states.

Yet another rule is less relevant to the Ukrainian struggle, but still important for the rest of the world. When the ultra-rich can hire mercenaries, they can wage war, no matter how small. States will no longer

be the only actors in war, and may even become trophies. Already today, international drug cartels are fighting each other for influence on the streets of Latin America. They are taking over countries such as Guatemala and calling them "drug states". Extractive industries, such as oil, gas, and mining companies, are increasingly turning to mercenaries to protect their people, territories, and property. Perhaps one day they will even fight each other over oil fields in weak states unable to defend themselves, or in states with corrupt politicians eager for bribes. Since firepower can be bought with money, the ultra-rich are becoming a new kind of superpower, and this portends wars without states. This rule explains what these wars will be like and what consequences they will have for international relations.

Rule 9. Shadow wars will prevail.

Russia seized Crimea in 2014 by means of shadow warfare — so it seemed to the international community, but not to Ukraine. In the information age, the capacity for creating convincing counter-narratives is a more decisive factor than military power on the battlefield. This drives war into the shadows, where it is fought in secret. Shadow warfare allows aggressors to ignite conflicts unnoticed, achieving victory before their victims even realize they have been attacked. Russia, Iran, and others have perfected the art of shadow warfare, and other states are following their example. Libya is one continuous shadow war: no one really knows who is on the battlefield and what they are fighting for. Meanwhile, the West does not understand the nature of shadow warfare, as evidenced by its muted response to Russia's actions in 2014. Modern states, including Ukraine, need to hone their ability to win shadow wars, and this rule explains how to achieve this.

Rule 10. Victory is fungible.

Understanding what victory looks like is half the battle. This rule offers Ukraine an excellent strategy for defeating Russia today: use time to your advantage. Brains are more important than brute force. As for brains, remember the Trojan horse and David versus Goliath. As for brute force, remember World War I. There are many ways to "win," and most do not require a huge army if you have brainpow-

er. You need a strategy that uses your enemy's way of waging war against them, just as a jiu-jitsu fighter uses their opponent's weight against them. This rule explains how to win in modern warfare.

In other words, the technological revolution already underway is creating ideal conditions for a war of attrition, and the strategy to achieve the war's political goal will aim to exhaust the enemy's resources and capabilities.

This conclusion allows us to identify the key and, probably, the only strategy for victory in the future: building a system of national resilience.

In his turn, the Ambassador Extraordinary and Plenipotentiary of Ukraine to the United Kingdom and Northern Ireland, Commander-in-Chief of the Armed Forces of Ukraine (AFU) V. Zaluzhny (2021–2024), points out that the Russian-Ukrainian war has completely changed the nature of war. Reconnaissance and strike drones, drones supporting artillery fire, and a situational awareness system have made the battlefield completely transparent. All this has provided unlimited opportunities for high-precision strikes at the tactical level. High-precision strikes on logistics routes have become commonplace today. Moreover, such strikes are already part of the tactics of pushing back enemy positions.

Consequently, absolute transparency in front of the front line has created a 10-15 km zone of complete destruction. It is no longer surprising when a drone hunts not for a group target or armored vehicle, but even for an individual soldier.

Why has this become possible? The reasons for this are:

First, the rapid development of electronic warfare (EW) capabilities. It is thanks to EW development that the ability of satellite technologies and radio- and GPS-guided munitions to deliver high-precision strikes at the operational level has been neutralized. The effectiveness of expensive missiles and high-precision shells has fallen to zero.

Second, a large number of visual reconnaissance and strike drones have appeared on the battlefield at the tactical and operational levels.

As a result, tactics and the art of operational command have undergone significant changes.

We can therefore confidently state that:

1. UAVs and digital technologies have rendered obsolete the conventional, familiar types of weaponry that have defined warfare for decades. They are now history.

2. Armored vehicles, which had been the basis of offensive operations since 1915, became defenseless against cheap drones and, as a result, are no longer used in other types of combat today.

3. GPS-guided high-precision weapons systems have lost effectiveness due to the development of electronic warfare.

4. Air defense (AD) is undergoing perhaps the most significant transformations. The emergence of a large number of small, cheap drones has made the use of expensive missiles for AD systems economically infeasible.

5. The skies above the battlefield are now inaccessible to crewed aircraft, rendering them an auxiliary means of AD. Aviation requires modernization and the ability to conduct reconnaissance and strike from completely different distances.

6. Naval drones gradually took over the seas. Powerful ships no longer venture beyond protected ports.

This is not just about technology. It requires a complete rethink of forms and application methods. As a result, military doctrine must be revised.

Evidently, Mr. Zaluzhny adds, winning on the battlefield now depends on the ability to outpace the foe in technological development. Changes are crucially needed along the chain "science (development) - production - application." Innovative development will depend on effective interaction between these elements. Of course, attention must be paid to:

1. The development of AI and machine learning. Apparently, the speed of AI implementation on the battlefield, especially in the management of complex processes across reconnaissance, planning, command, firepower, and autonomous combat systems (without human control), will provide a qualitative and quantitative advantage.

2. Electronic Warfare solutions. Perhaps this is above all. Essentially, two crucial tasks lie ahead: creating a digital domain for use and protecting it from enemy interference. Clearly, this involves searching for new communication technologies, such as cognitive radio. Such advances are already underway. It is also important to explore new navigation and guidance methods and to develop data transmission methods that extend beyond the radio frequency spectrum.

3. The development of inexpensive, high-precision, long-range unmanned systems. This increases the capacity for systematic destruction of enemy infrastructure, depletion of enemy air defense systems, and combined attacks on important targets.

4. The development and production of drones (robots) as a component of basic combat capabilities.

The Russian-Ukrainian war has taught countries an important lesson: war, which involves trading human lives for tactical gains, is no longer an option.

In modern combat, human beings are an extremely valuable resource. A resource that cannot be replaced. It is technology that allows combat effectiveness to be maintained while radically reducing losses.

Therefore, we must design:

- strike drones, which have proven their exceptional effectiveness, especially in conditions of artillery ammunition shortages;
- reconnaissance drones;
- anti-aircraft drones;
- ground-based unmanned systems;
- universal combat platforms;
- maritime unmanned systems.

5. Civilian or dual-use technologies have reached such a level of sophistication that they now form the basis of combat capabilities. These include:

- the use of commercial satellite systems for reconnaissance;
- the use of 3D printing for the rapid manufacture of spare parts and components for military equipment in improvised conditions;

- the use of social networks to gather intelligence;
- the creation of improvised electronic warfare systems from commercially available components to jam communications and control enemy drones;
- the use of civilian messengers with end-to-end encryption for data exchange;
- the use of cloud solutions.

Defense industries in leading countries today are following a trend (based on the principles and functional qualities of the Fourth Industrial Revolution) towards the development of force multipliers, complexes, and systems of weapons and military equipment (WME) that significantly surpass or will surpass existing weapons in terms of their capabilities (some countries have already commenced the adoption of such WME). Such models, complexes, and systems of military equipment and technology will be comparable in their combat characteristics and effects to high-precision weapons, including nuclear weapons. Correspondingly, attitudes toward the content, tactics, and strategy of armed conflict will change are changing – they are no longer seen as clashes between combat units that strike each other in the course of firefights and capture enemy territory, but as clashes between multifunctional combat systems, the main purpose of which is to deprive the opposing system of its ability to act [6].

Multifunctional, autonomous, and remotely controlled robotic systems (unified platforms) with AI, based on various architectures and applications, are being developed in real time for selective targeting of specific objectives from the tactical to the strategic level. Fundamentally new information-technical and information-psychological means of information warfare, as well as software and hardware tools for both conducting cyber operations and protecting against them, are emerging. Miniaturization has led to the development of small and ultra-small reconnaissance and combat-control devices, etc.

All this leads to a shift in the mutual influence of weapons and methods of warfare towards the latter's increasing dependence on

technology and the degree of weapon development. At the same time, it should be understood that, at the heart of any piece of equipment, lies the technology used to develop and manufacture it. Moreover, the "birth" of a new piece of equipment is determined by the emergence and mastery of new technological principles for processing raw materials, which allow the creation of the desired model in the future. The availability of basic technologies for the industrial production of technical equipment is a determining factor in the development of weapons [7].

For example, military scholars consider the following areas to be the most promising fields of application for nanotechnology, nanomaterials, and related products in ensuring national defense and security:

1. Cutting-edge design materials will significantly improve the reliability and operational range of current and future military equipment.
2. Means of reducing the visibility of various types of weapons.
3. Combat equipment for military personnel, designed to level up their protection, autonomy, and effectiveness.
4. Energy systems (materials) for weapons, mainly for various types of ammunition.
5. Compact and energy-efficient electronic component base for military use.

In addition, 3D printing is currently being actively used in the defense industry. Additive Manufacturing (AM), commonly known as 3D printing, has been identified by the European Commission as one of the key technologies capable of increasing industry competitiveness in Europe thanks to its capabilities for rapid, decentralized, and flexible production. AM is already being used in the civil industry and by defense manufacturers. However, the armed forces are still far from realizing the full potential of this technology. AM technologies strengthen defense capabilities. Forecast growth in the AM market is likely to yield multiple benefits for the defense community: reduced tooling and parts costs, improved design, shorter time-to-market, and enhanced technical and commercial competitiveness.

At the same time, 3D printing will significantly impact the maintenance of military assets by enabling the manufacture of spare parts and components. In addition, AM technologies may be promising for enhancing defense capabilities. These include logistical support for deployments in remote or hostile environments. These operational technologies can significantly affect the course of missions. The time between failures and the recovery of platforms, transportation, and storage for large quantities of supplies can be reduced, with a corresponding reduction in costs and the logistical burden on the operation.

The use of new materials for defense purposes is also a modern trend. Armaments and military equipment are becoming increasingly complex, as are the materials used to make them. In this context, advanced materials are of considerable concern, impacting the future operational effectiveness of military missions. Novel materials can be applied across a wide range of domains and hostile environments where risks and damage can be mitigated through protective solutions. It is expected that the most groundbreaking effects will be achieved through the integration of new developments, such as energy storage and applications, camouflage, personal health monitoring, and protection through "super-intelligent" materials for both platforms and soldiers. Other potential uses of new materials to be explored in the future include self-healing materials, cyber defense materials (for electromagnetic interference response), biometric material designs, morphing aerodynamic surfaces, and the integration of metamaterials.

The large-scale armed aggression of the Russian Federation against Ukraine has proven the relevance and primacy of military affairs and science for the development of Ukraine. In such conditions, the role and place of military science in ensuring national security, which should become one of the main factors in state building, are growing significantly.

2.2. The Concept of Russia's Mental Warfare

Recently, terms such as cognitive warfare, consciental warfare (CW), semantic warfare, discursive warfare, and mental warfare (MW) have become widespread. These terms are not completely interchangeable synonyms, although they describe the same phenomenon – the infliction of damage on the intangible components of military power: human will, spirit, conscience, etc. The term "mental warfare" most fully summarizes the essential characteristics of all the above definitions and conveys their semantic similarity.

According to the Encyclopedia of Modern Ukraine, mentality (from Latin *mens* – mind, way of thinking, disposition) is the perception and interpretation of the world in the spiritual life of a people, nation, or social entities [8]. Thus, MW is an invisible battlefield, because the struggle takes place primarily within a person, at the psychophysiological level.

Russia initiated MW against Ukraine long before the large-scale invasion of our sovereign state. According to experts, it is impossible to build an effective counteraction system without knowing the enemy's motivational mechanisms and real goals. In such a war, the victim reacts to the aggressor's tactical moves without understanding its strategy. This leads to the enemy always pulling the rug out from under your feet, because its actions are constant, repetitive, contradictory, and illogical.

In recent years, domestic and foreign experts have paid great attention to researching the goals, mechanisms, technologies, and means of Russian hybrid (in particular, information) aggression in Ukraine and Europe.

In fact, the battle for mindsets has been waged throughout the history of civilization. However, in modern conditions, as a result of the development of information technologies, changes in the mindset of the human personality and its cultural identification, as well as the destruction of the national historical values of society and the state, are becoming particularly intense and widespread.

According to Russian experts, the struggle for minds in modern warfare is aimed at achieving the following main goals [9–12]:

- Destroying the population's ability to understand the place and role of their country and its national strategy in order to develop complete indifference to the fate of the state and the people in the future.
- Destroying the mechanisms of traditional self-identification of the population and replacing them with new identification surrogates by involving people in various "participation and support groups" formed through social networks and the media.
- Lowering the general intellectual level of the population by forming "clip thinking," which does not involve a critical attitude toward the information presented.
- Introducing into the public consciousness a new, specially constructed matrix of values and norms of social and personal behavior as the only possible models of behavior. This leads to the destruction of people's ancestral, cultural, and historical memory, as well as to the psychotization and neurotization of society, which is transformed into a mob that is easily susceptible to external control by political manipulators.
- Eradication of issues from the information space of human consciousness that require thoughtful and unhurried reflection on events to form sustainable personal knowledge.

Today, the following techniques are used in mental warfare:

- Concealing critically important information about the state of affairs in various spheres of social life.
- Burying valuable information in a mass of "information garbage" according to the principle of "hiding a leaf in the forest."
- Substituting concepts or distorting their meaning.
- Diverting attention to insignificant events.
- Using terms that are commonly used in the media but whose meaning has been fundamentally altered.
- Presenting the audience with negative information that is more readily accepted than positive news.
- Discussing events that have no real social value and using the results of flawed sociological studies to create a distorted view of the situation in society.

- Introducing bans on certain types of information and news sections in order to prevent broad public discussion of issues and topics that are critical to certain power structures.
- Blatant lies aimed at misinforming the population of one's own country and the foreign public.

Some Russian military "experts" categorically assert: "When it comes to the Ukrainian army, there is a relatively small group of people who are fanatically devoted to the current Kyiv authorities and the neo-Nazi ideology that is the moral foundation of their rule. But there are others who have studied at NATO and American educational institutions. Their activities are well paid by the Kyiv authorities, and having established ties with representatives of Western elites and special services, they can count on a comfortable position in the West after completing their service or in the event of unforeseen circumstances. But in the event of a reorientation towards the East, they can obtain reliable guarantees from Russia and easily change their political orientation. Regarding the higher echelons of the Ukrainian army and navy, it is worth emphasizing the shaping of their perceptions of the possibility of preserving their lives and social status if they contribute to a change in Ukraine's political course. Based on the examples of Ukrainian Armed Forces servicemen who defected to Russia during the annexation of Crimea, it is worth emphasizing that Ukraine's top military leadership could have a more successful career, including in the ranks of the Russian Armed Forces. It is important to show the leadership of the Ukrainian army and navy that Western civilization, especially the US, is facing a serious crisis that threatens to break up the leading countries of this civilization, and, as a result, they are not concerned with Ukraine at the moment. They are only using the Ukrainian factor to put pressure on Russia."

These same "experts" cynically note: "As for the employees of the Ukrainian special services, who are overwhelmingly pragmatic but mostly uninformed in the field of geopolitics and international relations (with the exception of a limited group of specialists), it is advisable to focus efforts on proving simple things. First of all, that

for their Western masters, they are simply expendable material that can easily be sacrificed if necessary. There are plenty of examples of this, from Georgia to Afghanistan. They need to be told that if they help Ukraine shift eastward, even if only to a relatively small extent, for example, by remaining inactive or lenient towards pro-Russian citizens and organizations, they will not only avoid repression in the new Ukraine, but may also occupy higher positions, preserving and improving their social status.

It makes sense to follow a similar line of conduct with employees of the Ukrainian Ministry of Internal Affairs. They should be reminded of the humiliating position they find themselves in when militants from nationalist organizations, and sometimes outright criminals, are appointed and brought closer to the current Ukrainian authorities."

Regarding Ukrainian citizens, Russian "experts" are convinced that:

"The Ukrainian population is largely apolitical and intimidated, so the main emphasis should be placed on comparing the standard of living of the people in the union with Russia, especially during the Soviet era. It is necessary to demonstrate the futility of the current course, emphasizing the likely mass sale of land to foreigners. Show the prospect of the revival of the Ukrainian economy, even if independent, in partnership with Russia. Prove that the killing of their children, relatives, and loved ones will continue in any case, even if hypothetically the Donetsk People's Republic (DPR) and the Luhansk People's Republic (LPR) return into the fold of Ukrainian statehood, because without war, the current regime cannot exist. It is important that ordinary Ukrainians come to the conclusion that the current usurpers in Kyiv do not aim to revive Ukraine, but to destroy it, with the physical extermination of the vast majority of the Ukrainian population."

In conclusion, Russian representatives emphasize that the effectiveness of information warfare depends to a decisive extent on the diversity of efforts and resources involved in its conduct. To this end, all major state institutions and non-governmental entities should be involved, in particular:

- Official diplomatic state bodies that solve their own political, legal, and diplomatic tasks, as well as carry out special political and diplomatic actions.
- International non-governmental organizations whose main purpose may be to create a favorable international moral and psychological background for the state's activities, as well as to carry out specific information campaigns.
- State and non-state bodies and the media, which should be the main means of informational and psychological influence on the population and leadership of Ukraine;
- Political parties and movements, Christian and Islamic religious organizations, state and non-state cultural organizations and institutions, and creative organizations, which should be the most important factor in ideological, religious, and cultural influence;
- State infrastructure (energy, transport, and communications), the country's fuel, energy, and raw materials complex, and industry are the main instruments for implementing information campaigns using economic methods.
- State bodies and institutions that ensure the military, political, and internal security of the state: various special services and armed forces, as well as non-governmental paramilitary formations, play a major role in carrying out special information campaigns, particularly those of a demonstrative nature.
- Networking entities and communities in global cyberspace that have significant influence over the majority of Ukrainian society, especially young people. Of particular importance are those components located outside Russia that can act as foreign representatives, demonstrating alternative views on Ukraine from other countries.

Let us consider the structure and individual provisions of Russia's MW concept, its main patterns and principles.

According to Russian researchers, the new paradigm of war has the following features [10, 15]:

- Hostile actions (attacks) begin without warning, operate in gray areas, are evolutionary and permanent in nature, and often lead to the defeat of the victim state due to its inability to respond adequately.

- Defeated nation-states are eliminated, often without occupation of their territory, or lose not so much their population and resources as their political will and capacity for self-government.
- The population of the victim country often finds itself under the control of external and internal entities and loses the ability to control its own destiny.
- The struggle is for minds, knowledge, and will, for the worldview of individual citizens and society as a whole.
- National history, culture, traditions, institutions, and the population's life priorities are ignored and replaced by others imposed from outside, often with the tacit consent of the people.
- The occupation of spiritual space and public consciousness is considered a complete victory when the defeated not only lose the ability to defend their values but also fully assimilate the foreign and false ideas imposed on them by the victorious enemy who has asserted its will.
- The blitzkrieg in this war consists of paralyzing the enemy's will by influencing its elite and the media, and then using them to destroy state institutions and demoralize the army and security forces.
- The victim country is attacked not only from the outside, but also from within, which is radically different from the traditional method of conducting military operations "from the outside in." The fronts and battles of such a war are diverse in scale, but synchronized and systematic.

Russian military experts note that this new type of uncompromising geopolitical confrontation, with the characteristics described above, has been given a specific term: Mental Warfare. Characterised as total warfare in nature, this approach aims for a comprehensive influence on both the information sphere and the emotions, feelings, and moods of the population in the country facing aggression.

This leads to the definition of MW as a set of coordinated actions and operations of varying scale aimed at paralyzing the enemy's will, changing the individual and mass consciousness of the population, demoralizing the army and society, destroying spiritual and moral values, traditions, and the cultural and historical foundations of the state, and destroying national identity.

According to Russian experts, the mental struggle in modern warfare is aimed at achieving the following main goals [10–15]:

- Destroying the population's ability to understand the place and role of their country and its national strategy in order to develop complete indifference to the fate of the state and the people in the future.
- Destroying the mechanisms of traditional self-identification of the population and replacing them with new identification surrogates by involving people in various "participation and support groups" formed through social networks and the media.
- Lowering the general intellectual level of the population by forming "clip thinking," which does not involve a critical attitude toward the information presented.
- Introducing into the public consciousness a new, specially constructed matrix of values and norms of social and personal behavior as the only possible models of behavior. This leads to the destruction of people's ancestral, cultural, and historical memory, as well as to the psychotization and neurotization of society, which is transformed into a mob that is easily susceptible to external control by political manipulators;
- Eradication of issues from the information space of human consciousness that require thoughtful and unhurried reflection on events in order to form sustainable personal knowledge.

Russian experts [13] believe that the concept of MW should be considered an important component of general military theory (Fig. 2.1). The theoretical and methodological foundations of the MW concept consist of socio-philosophical, psychological, social, political, and other theories (e.g., the Overton window), national security theory, national security strategy, military science, the laws of war (the course and outcome of war, revealing their dependence on the economic, political, social, scientific, and military potential of the state), the laws of armed conflict, etc. The main place in the concept is occupied by philosophical and sociological provisions on the origin, essence, nature, and role of MW, as well as on the development and activities of the state and the armed forces in the context of such a war.

The structure of the concept of MW includes the following main sections: theoretical foundations; conceptual apparatus; methodological foundations (basic patterns of MW, methods and technologies of psychological defense); practical recommendations (Fig. 2.2). It is envisaged that the key provisions of the MW concept will subsequently form the basis for the development of relevant textbooks, manuals, guidelines, training course programs, practical and methodological recommendations for state and military authorities at various levels and higher education institutions.

The following main patterns of MW have been identified:

- Constant increase in intensity;
- Increasing comprehensiveness and persistence;
- Affecting all spheres of society (spreading like a cancerous tumor);
- Interconnection and mutual influence of all spheres of society and social institutions;
- The decisive nature of the mental domain and the significant influence of economic factors on the transformation of society.
- Delay in impact due to the inertia of consciousness (the complexity of counteracting MW techniques, because it is difficult, and sometimes impossible, to achieve the rejection of false beliefs imposed by the enemy), which creates problems in "curing" minds and transformations in the mental sphere of society that have resulted from the use of MW techniques.

Based on research into the experience and practice of applying various forms, methods, techniques, and approaches to conducting MW, certain principles have been formulated: preventiveness, relevance, adaptability, comprehensiveness, individuality, group and mass approaches, offensive nature, constant growth in intensity, and mirroring. Distorting reality is one of the main strategies of the Russian Federation and anti-Ukrainian forces in our country. An important component of anti-Ukrainian policy is the manipulation of historical discourse, which is used as a tool to level out Ukrainian identity, as well as the discrediting of the activities of the Armed Forces of Ukraine and its special services.

2.3. Trends in the Development of Information and Psychological Influences

The issue of the ontology of war has a long-standing tradition that dates back to antiquity. Since the time of the ancient Greek historian Thucydides, the methods of conducting war and the behavior of adversaries have received significant attention in studies of the nature of war. Many works from the post-Westphalian period focus on the essence of war as an antagonistic armed conflict between states aimed at achieving specific goals. The classic definition of war, articulated by the Prussian theorist Carl von Clausewitz as a means of achieving political objectives through other means, clearly outlines this understanding of the nature of war. While modern military theorists and practitioners do not fundamentally deviate from this classic definition, they are increasingly exploring the methods and technologies used in contemporary warfare.

Today, one of the most effective non-military weapons is information. War, as a means of communication, has become entirely digitalized and has evolved into a tool for dividing people. Ukraine was the first country in the world to confront digitalized military aggression.

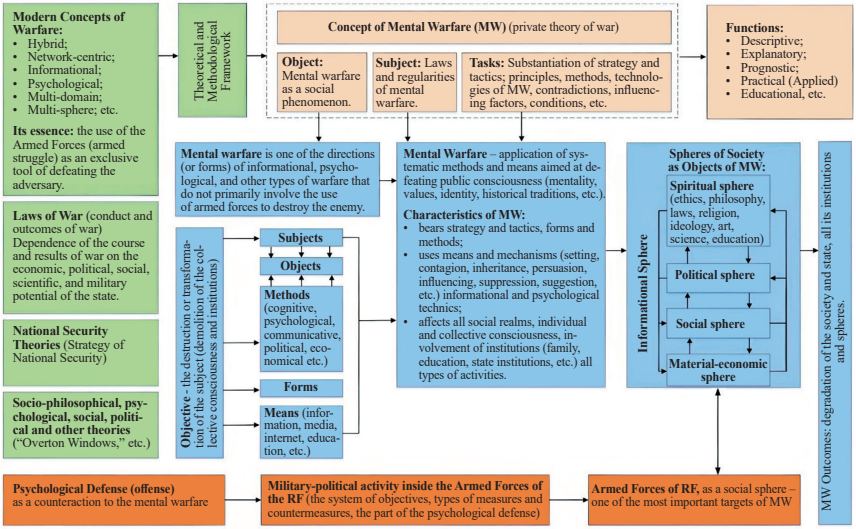

Fig. 2.1. The concept of MW as an important component in general military theory

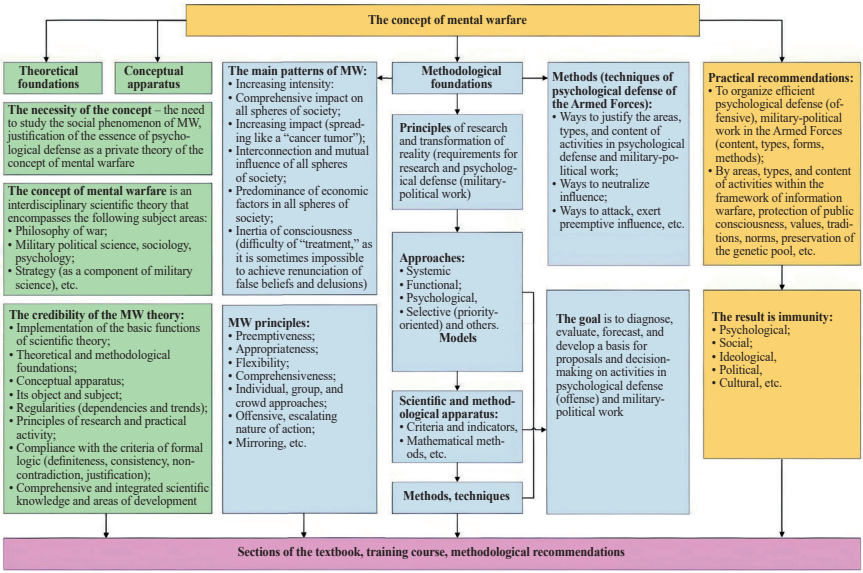

Fig. 2.2. Structure of the MW concept

H. Pocheptsov observes that information wars often do not differ significantly from one another, but they can be clearly categorized into technical and humanitarian types. Humanitarian information wars can be further divided into two categories: information wars and semantic wars. According to Pocheptsov, information wars focus on presenting new facts, while semantic wars aim to reinterpret existing facts. Semantic wars seek to dismantle the target's worldview, leading to decisions that the target would not have made under their previous worldview. Their methods may include not only direct tactics but also background influences and other subtle influencing operations.

The primary distinction lies in the long-term nature, allowing these actions to occur nowadays without the target being aware of the influence. As H. Pocheptsov points out, all wars are aimed at altering the behavior of the enemy or opponent, using various tools to achieve this. Each type of warfare targets a specific domain: conventional warfare focuses on physical space, information warfare on information space, and semantic warfare on cognitive space. Howev-

er, the Ukrainian experience has shown that the key focus of modern warfare is not cyberspace, but the cognitive domain.

If Hiroshima and Nagasaki became symbols of humanity's understanding of the destructive power of nuclear weapons, then Russia's war against Ukraine should become an example of understanding the danger of information weapons, namely information and psychological warfare.

There is a number of interpretations of information and psychological warfare in academic circles. The most accurate definition is that of researcher T. Bielska, who defines information and psychological warfare as the influence exerted with the aim of deliberately disseminating specific information that affects the psyche and behavior of the political elite and civil society of a particular country or region. Therefore, the highest form of warfare of the future can be called CW (Consciental War, from the Latin *conscientia* – consciousness) – a system of information, propaganda, and psychological measures carried out with the use of the media, culture, art, and other (psychotropic, psychotronic) means over a long period of time according to carefully developed scenarios.

After the large-scale invasion of Ukraine by the Russian Federation on February 24, 2022, a new phase of CW began, involving the use of a wide range of conscientious weapons and the experience gained in influencing people's consciousness through various information campaigns. The impact of such campaigns by the Russian Federation is aimed at three main target audiences:

- The audience of the country directly involved in the conflict – currently Ukraine (to shift value orientations, instill a worldview needed for emotional and psychological, and ultimately physical, subjugation, shape the public perception of the fairness of Russian leadership's decisions and plans).
- Russia's internal audience and the audience of countries that support it (to confirm the Russian leadership's actions are correct, to form the largest possible audience in support of the Kremlin's decisions, that not only sides with the propagandist, but effectively carries out its functions).

- The external audience (to create informational conditions for a favorable perception of Russian policy abroad, to create new agents of influence who, voluntarily, using levers specific to the audience of each country, will not only continue to support the Kremlin's ideology, but also incite Ukraine's allies to conflict).

D. Kashperska identifies the following as the main tools for conducting information warfare in cyberspace [16]:

- SMM activities (Social Media Marketing);
- Astroturfing;
- Deepfakes and substitution of reality;
- Suggestion on government websites, etc.

SMM activities. With the active development of social networks, another platform has emerged not only for selling goods, but also for selling ideas. The Russian Federation actively uses SMM capabilities and tools to exert informational and psychological influence on a wide social media audience. Social marketing tools in networks have many cases for managing consciousness and the choice of a particular object. Among the main principles of SMM used by the Russian Federation in its CW against Ukraine, the following can be distinguished: social proof, exchange, emotional trap, affection, authority, and scarcity.

Astroturfing. Modern cyber technologies enable the exertion of a suggestive influence not only through diverse content, but also through the active use of cyber simulacra. These are virtual accounts that simulate the representation of real people and, through comments on a particular piece of information, can change and distort its essence. This has led to the emergence of a special term, "astroturfing." The active use of the latest Internet technologies contributes to the replacement of social and political reality with computer simulations [17].

Astroturfing is the use of modern software or the purposeful hiring of paid users (so-called web brigades) to artificially control public opinion. This technology is used to suppress the opinions of real people on web forums and to organize fake online campaigns that create the impression that a large number of people are demanding something specific or opposing something.

The term comes from the name of the popular brand AstroTurf, which produces synthetic turf used instead of grass in stadiums. Over time, this term came to refer to the process of creating artificial public opinion, most often on the Internet, involving paid audience to participate in numerous forums, media sites, and blogs. They write sponsored content, leave comments under posts on social media, or mass-repost the desired information, thus creating the impression of spontaneous public support for a politician, political group or party, product, service, event, etc.

Since astroturfing is a form of cyber aggression, it is not only carried out by hired users. So-called trolls (commentators who add expressive color to the news), bots, fake accounts, and embedded banners with covert advertising created through the complex software circulate among them. A troll is creative, a bot is mechanical.

The main functions of astroturfing are as follows:

- Creating false perceptions of events and phenomena, suggesting false memories, etc.
- Manipulation (creating emotional and informational traps that impact decision-making, choice of a certain position, etc.).
- Creating a specific emotional backdrop for the audience (panic, fear, indifference, etc.).
- Provoking hostility and aggression (interethnic, racial, religious, etc.).
- Creating mass extracollective behavior (encouraging offline action).

Whereas bots mostly mechanically duplicate narrative specified by an algorithm, trolls create messages that use emotionally expressive vocabulary and evoke empathy in recipients.

According to a study by Princeton University (USA), Russia is responsible for 72% of disinformation operations in the world, including on social media, surpassing China, Iran, and Saudi Arabia [19]. Russia has been actively using astroturfing as part of its hybrid war against Ukraine since the Revolution of Dignity. The Russian government's use of astroturfing differs from traditional forms of propaganda. Its goal is not to convince or prove, but to undermine and discredit. On

the impact scale, it is classified as a weapon of mass destruction, not an instantaneous one, but rather a hidden, staged, pandemic-like information influence. The Kremlin actively uses bot farms to destabilize the socio-political situation in Ukraine and other developed democracies. The Oxford Internet Institute, part of the University of Oxford, analyzes the problem of cyberpropaganda in nine countries, including Ukraine [18]. The participants in this study, Samuel Woolley and Philip Howard, argue that after Euromaidan and Russia's annexation of Crimea, Ukraine has become the front line of numerous disinformation campaigns. Most of these campaigns have an online component that actively uses social media, trolls, and bots, which poses a number of specific internal and external threats to national security. According to the study, 21% of Ukrainians use social networks as their main source of news, while any social network can be a platform for active astroturfing aimed at spreading disinformation.

With the start of Russian aggression against Ukraine in 2014, Olgino trolls became active on various platforms within Ukrainian cyberspace. In 2017, the Russian social network VKontakte (VK) was banned and blocked in Ukraine. Until then, it had been the second most popular website after Google. Since the annexation of Crimea and the start of the "Russian Spring" in the eastern and southern regions, many politically oriented groups have been created to support the illegal actions of the Russian Federation on the territory of our country and spread anti-Ukrainian propaganda. Among the most well-known anti-Ukrainian groups of those years on VK, the following can be highlighted [19]:

- "Reports from the Militia of Novorossiya" [Сводки от ополчения Новороссии] by the notorious Igor Strelkov, who led the operation to capture Sloviansk in the spring of 2014 and has been an active YouTube blogger on military and political issues since February 2022, during the large-scale armed aggression of the Russian Federation.
- "Anti-Maidan" [АнтиМайдан] and other communities that have this word in their name.
- "People's Militia of Donbas" [Народное ополчение Донбасса].

- “Russian Spring” [Русская весна].
- “Donetsk Republic,” [Донецкая республика] etc.

At the end of 2018, the analytical platform VoxUkraine analyzed a database of nearly 4,000 Russian accounts published by Twitter October that year. They found that between 2010 and 2018, 1,369 accounts belonging to the Russian Internet Research Agency generated 774,957 tweets about Ukraine. These accounts had a total of 3.4 million followers. Before the annexation of Crimea, Russian bots on Twitter hardly touched on Ukrainian topics [20]. A gradual surge in their activity began after the sham referendum in Crimea.

One of the most striking cases of external cyber propaganda is the media activity in response to the crash of Malaysia Airlines flight MH17, which occurred in the uncontrolled territories of the Donbas on July 17, 2014, and claimed the lives of 298 people. According to one of the “conspiracy theories,” the plane was shot down in the air by a Ukrainian fighter jet. This version emerged from a Twitter post by Spanish air traffic controller Carlos (@spainbuca), who was allegedly tracking the flight. The user reported that he had observed two Ukrainian missiles near the plane seconds before a shotdown, additionally tweeting in series about Ukraine’s alleged responsibility for the disaster: “Kyiv is responsible,” “We are being threatened in the control tower,” “Before they take my phone away and smash my head in, once again: Kyiv shot down the plane.”

The post by @spainbuca went viral on the platform and was reposted by media outlets RT and TASS, as well as other Russian news agencies. In July 2014, these messages appeared at a press conference by the Russian Ministry of Defense. The Ukrainian Ministry of Information Policy later proved that this Twitter account was a bot, whose activity was initiated during Euromaidan to spread anti-Ukrainian slogans. In September 2016, a joint international investigation proved that the plane was shot down by a Russian Buk missile system from territory controlled by pro-Russian separatists.

In 2017, journalists from Radio Free Europe/Radio Liberty and a group of Romanian investigative journalists from the RISE Project reached out to a person named Jose Carlos Barrios Sanchez, who

had been posing as the user of this account during this period [21]. In conversation with them, he admitted that he had never worked as an air traffic controller and was not in Ukraine at the time of the MH17 crash. Sanchez claimed that he received large sums of money from Russia for his Twitter posts, specifically $48,000 from the media company RT, on which he later appeared after the Boeing was shot down. The TV channel denies ever having transferred money to Sanchez.

At the end of 2014, the account was reactivated but under the name Lyudmila Lopatyshkina. Like Spanish air traffic controller Carlos, she battles against the "Ukrainian junta" and retweets pro-Kremlin accounts, mixing this with meaningless messages ("fearless – watching," "I'll paint the sky," "he got it in '37"). This indicates that the "Lopatyshkina" account was a bot. By 2020, the account no longer exists.

Therefore, we can conclude that both during the period when the account was under the name Carlos and after it was renamed, it served as an artificial cyber simulacrum. However, in the first case, its activity was most likely controlled by a real person who set the agenda and intentionally provided false information to the audience. In the second case, posts on this page were made randomly, often containing grammatical and semantic errors, and retweets replicated those of the previous supposed owner of the Twitter account. It is worth noting that bots on the internet mainly follow and retweet each other. They may even be from different countries but speak the same language (Spanish, English, etc.). The example of the @spainbuca account confirms the effectiveness of astroturfing as a tool for political and social destabilization, which not only impacts citizens of one country (in this case, Ukraine) but also creates fake news stories for the entire global community.

Based on the analysis of such accounts, the following characteristic features of astroturfing can be identified:

- Anonymity.
- Significant mobilization potential, which contributes to the high social self-organization of citizens.

- Low financial costs for implementing information campaigns that attract widespread attention.
- High level of citizen loyalty to established communicators.

Rapid spread of fake information.

A characteristic feature of Russian cyber propaganda is that the Kremlin uses it both to shape reality in a given territory and to ensure the legitimacy of its armed forces' actions outside the country and influence the desired reaction of the international community and global military and political organizations, as demonstrated by the example of the @spainbuca bot account on Twitter.

The Russian Federation is equally active in using astroturfing ahead of elections in many EU countries. In September 2023, European Commission Vice-President Věra Jourová said that social media platforms need to act before the 2024 national and European elections to stop Russia's disinformation spread. She pointed out that X, formerly Twitter, which no longer follows the voluntary EU code of conduct, has the highest ratio of posts containing false information, thereby fueling Russia's "war of ideas," as noted in a Bloomberg article [22].

In the context of the Russian-Ukrainian war, the Kremlin uses any news hook for ideological influence. The cultural sector is no exception. Twitter (now X) provides a convenient way to influence the international community by accumulating a number of fake accounts that create information noise around a particular narrative. For example, during Ukraine's victory at Eurovision 2022, bots posing as European users spread a photo of the band Kalush, whose frontman appears to be making a gesture that resembles a Nazi salute. These insinuations align perfectly with the Russian Federation's goals of portraying Ukraine as a "Nazi" state to the world and its own people. Notably, these bots frequently follow pro-Russian accounts on Twitter, including Russia Today.

Journalists from The Conversation network discovered that at the start of the large-scale invasion, 75 official Russian government accounts were active, with a total following of over 7 million and more than 35 million retweets. Between February 25 and March 3,

2022, these accounts posted 1,157 tweets, approximately three-quarters of which focused on spreading false information about the invasion of Ukraine and attempting to justify it [23].

The large-scale invasion of Ukraine by the Russian Federation on February 24, 2022, sparked a new wave of bot activity. According to CASM Technology, a company researching online disinformation, February 24 experienced a peak in new Twitter registrations, which may suggest the organization of a network [24]. Also, after February 24, posts with hashtags such as #IStandWithPutin and #IStandWithRussia started appearing among the top posts on Twitter. When examining the accounts posting these hashtags, most were created either before the invasion in January-February or afterward. Notably, many accounts with semi-empty profiles are based in Africa and Asia. It appears that propaganda is also effective in India and Turkey, with the highest levels of suspicious account activity occurring in the first 12 days of the invasion.

Astroturfers, unlike automated bots, write meaningful texts, as confirmed by most studies by analytical companies. These are usually original posts with different wording. The practice of astroturfing is not new to Russia. When the global community faced the challenge of overcoming the new COVID-19 coronavirus strain during the pandemic, astroturfers around the world stepped up their activities, generating fake statements and spreading misinformation about the virus among the population through social networks [25]. In early July, King's College London released a study on how conspiracy theories and social media influenced people's behavior during the pandemic [26]. It states that individuals who primarily consume news on social media platforms like Facebook, Twitter, and YouTube are more prone to believe conspiracy theories about the pandemic. Russian bot farms mainly pick up fake news from well-known or little-known Russian media resources and engage in numerous reposts and retweets. Bot accounts also often publish only the introductory paragraph of an article, which, from a psycholinguistic point of view, must contain emotionally expressive vocabulary that helps to exert a suggestive influence on the recipient. According to a report by the

Security Service of Ukraine (dated June 1, 2020), since the beginning of the lockdown in Ukraine, more than 2,600 social media communities and accounts that spread fake news about COVID-19 have been blocked, 18 of which were acting on behalf of the Russian Federation [27]. The main messages of the troll account bots were calls to violate lockdown restrictions, protest, seize power by force, and support such illegal actions.

Researchers at Carnegie Mellon University say that bot campaigns have dominated many online conversations about the coronavirus since January, i.e., since the very beginning of the pandemic. After analyzing more than 200 million tweets on the topic of coronavirus, researchers found that approximately 82% of the top 50 influential retweets were bots, and 62% of the top 1,000 influential retweets were also bots [28]. So, astroturfing is a way of distorting reality by placing the necessary emphasis on a particular information campaign on social media through a large number of reposts or posts with similar content, third-party comments under the post, or in microblogs that change the essence of the post itself, news, events, etc. The main components of this type of cyber propaganda are bots and trolls. Their main tasks are to instill feelings of panic, fear, indifference, hatred, or aggression, and to transform attitudes toward facts and personalities, etc. In the era of active Internet communication, manipulating consciousness with the tools of information messages from bots and trolls is one of the main ways of waging hybrid warfare, as well as providing information support for Russia's large-scale aggression against Ukraine. According to the Oxford Dictionary, manipulation is controlling or influencing a person or situation, often in a dishonest way [29].

Trolling is one form of astroturfing, in which information is presented or commented on in an aggressive or humorous manner. Other people often perceive aggression as confidence in one's position, which most often dulls the listener's/reader's vigilance and desire to verify the accuracy of the information. The effectiveness of astroturfing has been increased by adapting bot technology to its tasks – special programs that perform any actions automatically or

according to a set schedule/algorithm through the same interfaces as a typical user.

Alongside popular social media platforms among Ukrainians, such as Facebook, Instagram, and YouTube, the Telegram messenger is becoming increasingly popular, offering social media features, including blog pages. This application, created by Russians Nikolai and Pavel Durov, already has half a billion users. It is among the 10 most popular mobile applications worldwide. Telegram's popularity was fueled by disputes with Roskomnadzor, which tried to access data or block the messenger in Russia. The Telegram team has repeatedly publicly rebuffed the Russian special services, drawing in new users. Telegram allows users to create channels where owners can unilaterally distribute public content; the information in these channels is open to anyone, and anyone can subscribe to them. In Ukraine, anonymous Telegram channels have become popular, spreading disinformation and manipulating facts, and they have clear links to Russian propaganda media and special services [30]. The main reasons why Telegram is a favorable platform for conducting CW are as follows:

- End-to-end encryption and the ability to communicate with an unlimited number of people;
- Lack of clear content moderation policies and procedures;
- Complete anonymity;
- Ease of creating and administering channels;
- Customizable instant notification system, etc.

Both on social media platforms and information portals, propagandists use classifiers — a system that categorizes disinformation messages into groups based on predetermined criteria. Classifiers are keywords that match variants of disinformation messages (narratives).

For example, the following classifiers can be recalled:

- "Kalibr" (typical variants of reports in Russian news: high-precision weapon; unparalleled cruise missile; weapon of victory);
- "Ukrainian authorities" (typical variants of reports in Russian news: the Kyiv regime; Zelenskyi's authorities; the Kyiv junta, the Ukrainian Reich);

- "Patriots of Ukraine" (typical variants of reports in Russian news: Bandera supporters; nationalists; neo-Nazis; Azov members; the Kyiv army);
- "HIMARS" (typical examples of reports in Russian news: American multiple launch rocket system; inaccurate and outdated weapon; has a short range; kills civilians).

To enhance the semantic and emotional impact, classifiers are paired with relevant video footage in the news.

Deepfake and the substitution of reality. The era of "deep" fakes with multiple realities has created a matrix of information in which the individual becomes not only a consumer but also an element of this system. Internet users multiply the number of interpretations, and thanks to modern digital technologies, they can create an alternative reality that is almost impossible to recognize as fake immediately. Considering the fastest rise in information consumption driven by clip thinking, deepfake technology has developed as a product of AI technology, leading to the surge of fake video and audio recordings worldwide. As AI gets more advanced, the new fakes appear more convincing.

This technology is gradually changing the rules of the game in the field of political tactics and information warfare. Deepfakes are becoming a national security issue of a new generation. The creation of fake news and malicious deception, including discrediting celebrities and public figures and destroying political reputations, is all happening thanks to this technology with the greatest effectiveness, since consumers have almost no time for in-depth analysis amid the rapidly changing flow of information, especially in times of heightened social tensions. The ability to spread information, or spreadability, which American researcher Henry Jenkins wrote about in 2013 in his book Spreadable Media [31], has a negative impact on perception and awareness — users are, on average, inclined to click the "share" button without thinking, relying primarily on the attractiveness and virality of the content rather than its authenticity. Therefore, deepfakes have become a real shock technology, against which there is no perfect protection yet — only critical thinking and fact-checking.

There are already many applications on the global market that anyone can use to make a deepfake. The most famous of these are Zao, DeepFaceLab, and Deepfakes web β. Sam Gregory, program director of the American non-profit organization Witness, notes that deepfakes are often used to discredit female journalists and social activists. However, according to his observations, politicians have begun to frequently use deepfakes as an excuse for unsuccessful speeches or inadvertently uttered phrases in the public sphere that have caused a stir. They claim, "it's a deepfake, " which is equivalent to "it's fake news" [32].

This technology first caused a major political stir in 2020. The situation concerned the Extinction Rebellion social and political movement (Belgium), which used deepfake technology to "force" Belgian Prime Minister Sophie Wilmès to say that the cause of the coronavirus was environmental problems. Another high-profile case involved the falsification of a video speech by U.S. House Speaker Nancy Pelosi, in which an effect was added to make her appear drunk. This video was viewed by more than 2.5 million social media users online. However, the most famous fake video was a doctored speech by Barack Obama, in which he used foul language to address Donald Trump. Millions of people watched this video on YouTube and heard words from the president that he never said. There was no scandal, as the director of this montage, Jordan Peele, appeared on camera and explained that he was trying to draw attention to digital disinformation with this creative stunt.

Russia is currently only beginning to explore the possibilities of this technology. A classic example of deepfake is the case when, in 2017, the Russian Ministry of Defense published several posts on Twitter and Facebook containing "irrefutable evidence" of the U.S. cooperation with ISIS militants. Instead, it was a cropped screenshot from a promo for the mobile game AC-130 Gunship Simulator, along with a video of the Iraqi Air Force (IAF) eliminating ISIS militants in 2016.

Since the beginning of Russia's large-scale invasion of Ukraine, the Centre for Countering Disinformation has warned citizens on Facebook about a possible digital provocation by the Kremlin (deep-

fakes), in which Volodymyr Zelenskyi would announce the country's surrender [33]. The purpose of such a video is to disorient, sow panic and a sense of despair among citizens, demoralize the country's special services, and persuade the troops to lay down their arms. Although this scenario was not executed concerning the president, deepfake technology was successfully employed in June 2022 to discredit Kyiv's mayor, Vitali Klitschko. It was reported that several European capitals received requests from a fake email address to communicate with him via the ZOOM app. The mayors of Berlin and Madrid agreed to talk. Thanks to this technology, hackers used Klitschko's appearance for negotiations. Deutsche Welle reported that in a conversation with Berlin Mayor Franziska Giffey, the fake Klitschko talked about social benefits for Ukrainian refugees and asked for measures to be taken to encourage young men to return to Ukraine to fight. The interlocutor also asked for support for Kyiv with advice on holding an LGBT pride march [34]. This conversation contained typical Kremlin narratives, which point to a Russian trace in this fake conversation. But the propagandists made a big mistake — they built the conversation solely on constructs that elicit a response instead of making it more emotionally/psychologically intertextual and suggestive. As a result, the mayor herself later questioned the authenticity of this conversation. It is worth noting that this is the first case of deepfake being used in live online communication at a high international level, affecting not only the reputation of a political figure but also that of the entire country.

Suggestion on government websites. One of the most hidden forms of conscientious influence, in terms of its mechanism and chosen platform, is the suggestion of attitudes and perceptions of certain facts of the country's socio-political life through the open communication channels of government websites, in particular the electronic petitions page on the website of the President of Ukraine [35].

One feature of direct democracy is the right of citizens to submit written appeals to state authorities, thereby directly participating in state governance and shaping the country's policies across various fields. One such instrument of the voice of the people (vox populi) is

electronic petitions (e-petitions), which were introduced on the website of the President of Ukraine in August 2015. Within three months, a petition must collect at least 25,000 votes, and then the president is obliged to respond to it within 10 days.

E-petitions serve several functions. First, they make it possible to put a particular issue on the agenda. Second, petitions can be used to propose solutions to the issues raised, thereby involving citizens in the decision-making process. Third, petitions stimulate horizontal communication between citizens themselves, because in order to collect the required number of signatures, the initiators must persuade others to support the petition. Thus, raising awareness of an issue, bringing an author's idea to the attention of the public, and involving (often virally, using SMM tools) a large number of citizens in the discussion is a fairly convenient mechanism for managing public opinion, and, thanks to the various textual content of the appeals themselves and the consciousness of the individual, hidden means through the channel of official communication between the authorities and citizens. That is why electronic petitions are of considerable interest, given their potential for conscientious influence in the context of Russia's war of meanings and information war against Ukraine.

Despite the fact that Article 23-1 of the Law of Ukraine "On Citizens' Appeals" [36] stipulates that a petition "may not contain calls for the overthrow of the constitutional order, violation of the territorial integrity of Ukraine, propaganda of war, violence, cruelty, incitement of interethnic, racial, religious enmity, calls for terrorist acts, infringement of human rights and freedoms," there remains considerable scope for more covert manipulation. Such texts become an active tool for promoting Russia's interests in Ukraine through agents — Ukrainian citizens (only Ukrainian citizens with an electronic signature can submit a petition). Based on this, we can classify the following types of dangerous petition content, taking into account the audience they target:

- Manipulation of information, distortion of the information field, imposition and artificial suggestion of public opinion, creation of the illusion of the relevance of a particular issue through infor-

mation noise, and trust in state electronic resources, as well as the promotion of non-Ukrainian discourse.

- The adoption by certain forces in power of practical decisions that are questionable for the state on the basis of public appeals, which undermines the foundations of national security.

In 2020, the news agency Kırım Haber Ajansı (Crimean News) conducted a content analysis of petitions on the website of the President of Ukraine on the topic of Crimea and found that after the official cessation of electricity supplies to the peninsula on January 1, 2016, many petitions began to be written poorly, with a significant number of spelling and stylistic errors, without serious justification for the proposal, and even mixed with Russian [37]. The study showed that a fairly large number of petitions called for various ways to de-occupy Crimea and tocut off the peninsula's land connection with the mainland. Each time these petitions appeared in the Russian media and on Ukrainian social media, they were actively promoted and discussed. Russia interpreted the issue of "cutting off" Crimea as Ukraine's de facto recognition of the occupation of Crimea in perpetuity.

During the new phase of the Russian-Ukrainian war, which began on February 24, 2022, a number of provocative petitions were registered, in particular on defense issues, namely:

- A request to raise the age of mobilization for men to 65 and to abolish compulsory military registration for women. This petition sparked heated, ambiguous discussions among Ukrainian citizens on social media, and the Russian media used this to support two theses: "Ukraine has a shortage of manpower" and "Ukrainians do not want to carry out the criminal orders of the Kyiv regime."
- Requests for permission to travel abroad for men of various categories during martial law. The Russian Federation uses these regular petitions to deepen divisions and hostility within the Ukrainian community in order to prevent its consolidation against a common enemy.
- Multiple petitions received almost daily regarding the urgent provision of heavy weapons to the eastern front of Ukraine. The prevalence of such content creates panic among Ukrainian citizens by

constantly imposing the idea of betrayal, and is also used by agents of influence to emphasize Ukraine's inability to resist the "might of the Russian army."

- Calls for a peace agreement with Russia. Most of these petitions are not constructive, but rather emotionally expressive appeals that instill a sense of despair and convince people that the war could be ended right now, but that it is not in someone's interest to do so, and that the authorities do not care about the people.

It can be argued that the petition filtering system used for publication is quite weak and needs revision. The content itself should also be the focus of in-depth scientific research, along with close oversight from authorized law enforcement agencies and special services of Ukraine, particularly the intelligence agencies. Flooding the service with petition spam, in which constructive ideas and proposals are lost, and the mechanism of interaction between the authorities and the community is discredited, is an example of a technology of hybrid warfare that Russia is waging against Ukraine. The technology of reflexive management of the enemy's behavior is used, which leads to the undermining of the authority of government institutions and democratic institutions, and damages the image of the institution of the presidency as such, the Verkhovna Rada of Ukraine, the Cabinet of Ministers of Ukraine, etc. Petitions carry a danger that lies in their practical implementation: providing grounds for the actions of Russian agents of influence in power and the actions of people who are not deeply involved in a particular issue.

Given the above, it can be assumed that digital consciental attacks on Ukraine will only increase. This will require the development of new methods of counteraction, as well as interdisciplinary approaches to working with information on the internet and establishing close connections at the national level with global IT companies such as Google, Meta, and Microsoft. The effectiveness of such cooperation became evident after these companies' report in September 2023. At the request of the European Union, namely the President of the European Commission, they analyzed their information space for the share of Russian propaganda and disinformation related to Russia's war against Ukraine.

The companies operate under a Code of Practice, to which Alliance4Europe, Newtral, EFCSN, and Seznam have become signatories. The signatories, which are large online platforms, have committed to reporting on their activities every six months. The reports contain information about the platforms' actions to reduce disinformation surrounding the topic of Russia's war in Ukraine. TikTok and Meta have expanded their fact-checking efforts in various EU languages. They also collaborate with news agencies, including Reuters. Meta's fact-checking covers 22 EU languages, including Czech and Slovak, as of today. TikTok fact-checks content in Russian, Ukrainian, Belarusian, and 17 European languages. It reviewed 832 war-related videos, after which 211 were removed.

It has been noted that 30% of users change their minds about sharing a post when they see the label "unverified content" [38].

Given the serious risks posed by disinformation to European democracies, the commission expects signatories to step up efforts to combat disinformation in Ukraine and ahead of the European elections. In light of this, it would be appropriate for the Ministry of Digital Transformation of Ukraine, in particular, to join these initiatives as a stakeholder and gain access to the Transparency Center's archive, where reports are stored. It should also work with these companies to expand information verification efforts, even by involving Ukrainian news agencies in the collaboration. This approach would allow the government to gain partial control over digital propaganda infrastructure, make the most of the capabilities of the information-networked metamodern society, and, through digital technologies, prevent the replacement of the real world, genuine ideas, and beliefs with artificial simulacra created by the aggressor.

Conclusions to Section II

The Russian-Ukrainian war could end soon or it might last for years. In any case, it has already revealed what future wars will look like, much like how the civil war in Spain foreshadowed World War

II. Ukraine can defeat Russia just as David defeated Goliath. There are many ways to win, and a clever strategist knows how to implement them.

Ukraine has thwarted Russia's offensive plans. The actions of the Armed Forces of Ukraine in repelling Russia's large-scale aggression have been officially described as a series of coordinated operations. The details of these operations will be described by historians. However, some paradoxes of the Russian-Ukrainian war can already be pointed out, which came as a real surprise to most countries in the world:

- No modern army has ever been involved in a war of such high intensity. The war that Russia unleashed against Ukraine has become the largest conflict in Europe since World War II. Ukraine is fighting on equal terms with a nuclear power and an army that Russian propaganda until recently described as "second in the world."
- Ukraine's successes on the front lines, supported by numerous allies, have caused China to suspend its plans to invade Taiwan.
- The Armed Forces of Ukraine have rapidly mastered high-tech foreign-made weapons and military equipment. At the same time, Ukraine is actively reviving its defense industry.
- Despite having virtually no modern navy, Ukraine is defeating the Russian Black Sea Fleet, transforming its operational-strategic capabilities into operational-tactical ones (at the flotilla level).
- The offensive actions of the Armed Forces of Ukraine have refuted one of the fundamental postulates of military science about the need for a numerical (3-5 times) superiority in manpower and weapons during an offensive. The Ukrainian army is advancing despite the enemy's superiority in both weapons and personnel.
- Ukrainian logistics, parts of which are located abroad, meet most of the front's needs. They have been successfully optimized to address the threat of air and missile strikes.

Considering today's realities, military science must offer a forward-looking scientific and theoretical foundation for current national security issues, open up opportunities for military development, and ensure that innovations are rapidly adopted in the activities of

the Armed Forces of Ukraine — including training, deployment, and support.

The Russian army's attitude towards civilians is fundamentally at odds with the principles of modern military culture, suggesting that the Russian army's leadership is deliberately rejecting the humane methods of warfare mandated by international law. The information war that Russia is waging against Ukraine, alongside its conventional war, is just as aggressive and destructive. Russia's information and propaganda efforts are causing enormous damage to the mental health of the Ukrainian people. Recent studies conducted on Ukrainian society show that levels of mental disorders, trauma, and illness among the population have risen sharply during the period of Russian aggression.

People who have a history of mental disorders, as well as young people and the elderly, are particularly vulnerable to the negative effects of information operations and propaganda campaigns. Aggressive information and propaganda campaigns cause various mental disorders among the Ukrainian population, the most common of which are post-traumatic stress disorder, anxiety disorders, depression, and suicidal thoughts. The growing amount of disinformation, fake news, and manipulative information campaigns is a serious challenge to the mental health of citizens. Information aggression, particularly in the context of the modern information age, can affect the psychological state of all categories of the population without exception, including both military personnel and civilians. Various preventive and remedial approaches, methods, and technologies can help citizens maintain their mental health.

In today's world, information warfare is one of the decisive factors in victory. This is especially important for Ukraine, which is waging an asymmetric war against a nuclear power with superior military capabilities. The level of political support, the amount of aid, and the scale of sanctions imposed against the aggressor depend on how events in Ukraine are perceived abroad.

Today, there is a process of radical rethinking of the established image of information and the essence of information wars, their goals,

and methods. This is particularly acute in the Russian Federation's foreign policy towards Ukraine and during the full-scale Russian military aggression in 2022. The Russian Federation uses psychological operations and disinformation, which has become a standard and integral practice of "hybrid" warfare – the Kremlin's foreign policy on a global scale. The events unfolding in Ukraine are the greatest test in the entire history of Ukrainian statehood. Russia continues to use active forms of information and psychological influence and overt propaganda against Ukraine in order to consolidate its own population, destabilize the internal situation in our country, and "legitimize" its aggressive actions on the international stage. In order to understand how Russia is waging its information war, it is necessary to understand the manipulations it is resorting to. The directions and methods of Russia's information wars against Ukraine have been and remain:

- Gradual deterioration of Ukraine's international image with the aim of weakening its geopolitical significance.
- Appropriate dosing and distortion of information with the aim of destabilizing the situation in the state and implementing its own policy of "controlled chaos."
- Forming a stereotype of inferiority and secondary importance of Ukrainians, as well as the corresponding destruction of the sense of nationhood and peoplehood.
- The dominance of the Russian language, culture, and traditions to establish self-identification while simultaneously displacing the Ukrainian language and culture.

References:

1. Seredin, A. (2023, March 8). Viina v Ukraini yak viina piatoho pokolinnia: Chomu tsia viina ne pereroste u Tretiu svitovu [War in Ukraine as a fifth-generation war: Why this war will not escalate into World War III]. *Politychna Teolohiia*. https://politteo.online/materialy/vijna-v-ukrayini-yak-vijna-pyatogo-pokolinnya-chomu-czyavijna-ne-pereroste-u-tretyu-svitovu/ (Accessed July 25, 2025)

2. Kobets, Yu. (2024). Osoblyvosti rozhortannia ta typolohizatsiia sposobiv vedennia suchasnoi viiny [Features of deployment and typologization of ways of modern warfare]. *Visnyk Prykarpatskoho universytetu. Seriia: Politolohiia*, (17), 59–66.

3. Trebin, M. P., & Chernyshova, T. O. (2024). Trendy zbroinoi borotby u viinakh XXI stolittia [Trends of armed struggle in the wars of the 21st century]. In V. A. Krotiuk (Ed.), *Svitohliadnyi sens suchasnoi viiny: sociohumanitarni aspekty* (pp. 200–236). Kharkiv: KhNUPS.

4. McFate, S. (2023). *Novi pravyla viiny. Peremoha v epokhu khaosu* [The New Rules of War: Victory in the Age of Durable Disorder] (I. Bihun, Trans.). Kyiv, Ukraine: Nash Format. (Original work published 2019)

5. Zaluzhnyi, V. (2025, April 25). *Nova pryroda viiny zminyla sutnist osnov hlobalnoi bezpeky: ukrainskyi dosvid i maibutnii svitovyi poriadok* [The new nature of war has changed the essence of the foundations of global security: Ukrainian experience and the future world order]. https://www.pravda.com.ua/columns/2025/04/25/7509135/ (Accessed May 14, 2025)

6. Koval, V. V., Semenenko, O. M., Skurinevska, L. V., Mokliak, S. P., Tkach, I. M., & Yasenko, S. V. (2023). *Teoretychni zasady upravlinnia oboronnymy resursamy* [Theoretical foundations of defense resource management] (O. M. Semenenko, Ed.). Kyiv, Ukraine: General Staff of the Armed Forces of Ukraine.

7. Defense Express. (2020, November 14). *10 trendiv maibutnoho, yaki armiia Ukrainy poky shcho ihnoruie* [10 trends of the future that the Ukrainian army is still ignoring]. https://defence-ua.com/minds_and_ideas/10_trendiv_majbutnogo-2067.html (Accessed January 24, 2025)

8. Hrabovska, I. M., & Hrabovskyi, S. I. (2025). Mentalnist [Mentality]. In I. M. Dziuba, A. I. Zhukovskyi, M. H. Zhelezniak et al. (Eds.), *Entsyklopedia Suchasnoi Ukrainy* (Online ed.). Institute of Encyclopedic Research of the NAS of Ukraine. https://esu.com.ua/article-66534

9. Ilnitskiy, A. M. (2021). Mentalnaya voyna Rossii [Mental war of Russia]. *Voyennaya mysl*, (8), 19–34.

10. Marichev, M. O., Lobanov, I. G., & Tarasov, Ye. A. (2021). Borba za mentalnost – trend sovremennoy voyny [The struggle for mentality – a trend of modern war]. *Voyennaya mysl*, (8), 48–56.

11. Sivkov, K. (2021, November 2). Tekhnolohiia vrazumlennyia. Kak ubezhdat naselenye Ukrayny v neyzbezhnosty dobrykh otnoshenyi s Rossyei [Technology of admonition. How to convince the population of Ukraine of the inevitability of good relations with Russia]. *Voenno-Promyshlennyi Kurer*, (42). https://vpk.name/news/553966_tehnologiya_vrazumleniya.html

12. Manoylo, A. (2021, October 20). Rytsary plashcha y provokatsyy. Informatsyonnyie operatsyy razvedok evoliutsyonyruiut y obretaiut novyie formy [Knights of the cloak and provocation. Intelligence information operations evolve and take on new forms]. *Voenno-Promyshlennyi Kurer*, (40). https://vpk.name/news/550524_rycari_plasha_i_provokacii.html (Accessed December 10, 2025)

13. Karavayev, I. N. (2022). Kontseptsiya mentalnoy voyny kak sostavnaya chast ucheniya o voyne i armii [The concept of mental warfare as an integral part of the doctrine of war and the army]. *Voyennaya mysl*, (3), 35–42.

14. Ilnitskiy, A. M. (2022). Strategiya mentalnoy bezopasnosti Rossii [Strategy of mental security of Russia]. *Voyennaya mysl*, (4), 24–35.

15. Korzhevskiy, A. S., & Solovyov, I. V. (2022). Mentalnoye protivoborstvo i problemy formirovaniya tselostnoy sistemy nastupatelnykh i oboronitelnykh deystviy v nem [Mental confrontation and problems of forming a coherent system of offensive and defensive actions in it]. *Voyennaya mysl*, (11), 32–42.

16. Myronenko, P. V., & Mokliak, S. P. (Eds.). (2024). *Hrani ahresii: deiaki uzahalnennia dosvidu rosiisko-ukrainskoi viiny 2014–2024 rokiv* [Facets of aggression: some generalizations of the experience of the Russian-Ukrainian war of 2014–2024]. Kyiv, Ukraine: Politiia.

17. Sviderska, O. I. (2019). Formuvannia virtualnoho natovpu shliakhom manipuliatsii svidomosti naselennia [Formation of a virtual crowd through manipulation of public consciousness]. *Hileia: Naukovyi Visnyk*, (149), 62–66.

18. Martin, D. A., Shapiro, J. N., & Greene, K. T. (2024). *Trends in online foreign influence efforts* (Research Report). Empirical Studies of Conflict Project, Princeton University. https://esoc.princeton.edu/publications/trends-online-influence-efforts (Accessed August 24, 2025)

19. VKontakte. (2024). *VKontakte* [Social Network Service]. https://vk.com (Accessed August 17, 2024)

20. VoxUkraine. (2025). *Kak rossiyskaya «Fabrika trolley» pytalas vliyat na povestku dnya v Ukraine. Issledovaniye 755 000 tvitov* [How the Russian "Troll Factory" tried to influence the agenda in Ukraine. A study of 755,000 tweets]. https://voxukraine.org/longreads/twitter-database/index-ru.html (Accessed August 27, 2025)

21. The Insider. (2023, July 17). *Ispanskiy dispetcher, videvshiy, kak ukraintsy sbili MH17, prevratilsya v Lyudmilu Lopatyshkinu* [Spanish air traffic controller who saw Ukrainians shoot down MH17 turned into Lyudmila Lopatyshkina]. https://theins.ru/antifake/27246 (Accessed July 17, 2023)

22. Bloomberg. (2023, September 26). *Musk's X Is Biggest Outlet of Russia Disinformation, EU Says*. https://www.bloomberg.com/news/articles/2023-09-26/eu-faults-musk-s-x-in-fight-against-russia-s-war-of-ideas (Accessed September 30, 2023)

23. The Conversation. (2023, September 26). *Russian Government Accounts Are Using a Twitter Loophole to Spread Disinformation*. https://theconversation.com/russian-government-accounts-are-using-a-twitter-loophole-to-spreaddisinformation-178001 (Accessed September 26, 2023)

24. CASM Technology. (2023, September 26). *#IStandWithRussia #IStandWithPutin: Message-based community detection on Twitter* (Research Report). https://files.casmtechnology.com/message-based-community-detection-on-twitter.pdf (Accessed September 26, 2023)

25. Kashperska, D. O., & Karpenko, A. V. (2020). Vplyv astroturfinhu na natsionalnu bezpeku pid chas pandemii koronavirusu COVID-19 [The impact of astroturfing on national security during

the COVID-19 coronavirus pandemic]. In *Spilni dii viiskovykh formuvan i pravookhoronnykh orhaniv derzhavy: problemy ta perspektyvy* [Joint actions of military formations and law enforcement agencies of the state: problems and prospects]: Proceedings of the International Scientific and Practical Conference (pp. 278–279). Odesa, Ukraine.

26. Allington, D., Duffy, B., Wessely, S., Dhavan, N., & Rubin, J. (2021). Health-protective behaviour, social media usage and conspiracy belief during the COVID-19 public health emergency. *Psychological Medicine*, *51*(10), 1763–1769. https://doi.org/10.1017/S003329172000224X

27. Security Service of Ukraine. (2021, January 13). *U 2020 rotsi SBU neitralizuvala 600 kiberatak i vykryla 20 khakerskykh uhrupovan* [In 2020, the SBU neutralized 600 cyberattacks and exposed 20 hacking groups] [News post]. https://ssu.gov.ua/novyny/u-2020-rotsi-sbu-neitralizuvala-600-kiberatak-i-vykryla-20-khakerskykh-uhrupovan

28. Carnegie Mellon University. (2020, May 20). *Nearly half of the Twitter accounts discussing 'reopening America' may be bots*. https://www.cmu.edu/news/stories/archives/2020/may/twitter-bot-campaign.html (Accessed February 13, 2026)

29. Oxford University Press. (n.d.). Manipulate. In *Oxford learner's dictionaries*. https://www.oxfordlearnersdictionaries.com/definition/american_english/manipulate (Accessed September 26, 2023)

30. Security Service of Ukraine. (2021, February 1). *SBU vykryla ahenturnu merezhu spetssluzhb RF, yaka destabilizuvala sytuatsiiu v Ukraini cherez Telegram-kanaly* [The SBU exposed an intelligence network of the Russian special services that destabilized the situation in Ukraine through Telegram channels]. https://ssu.gov.ua/novyny/sbu-vykryla-ahenturnu-merezhu-spetssluzhb-rf-yaka-destabilizuvala-sytuatsiiu-v-ukraini-cherez-telegramkanaly (Accessed June 12, 2021)

31. Jenkins, H., Ford, S., & Green, J. (2013). *Spreadable media: Creating value and meaning in a networked culture. New York, NY*: New York University Press.

32. WIRED. (2019, October 4). *Researcher explains deepfake videos* [Video]. YouTube. https://www.youtube.com/watch?v=u2lX-70U7N0c

33. Center for Countering Disinformation. (2022, March 20). *Uiavit, shcho bachyte v televizori Volodymyra Zelenskoho…* [Imagine seeing Volodymyr Zelenskyy on TV...]. Facebook. https://www.facebook.com/protydiyadezinformatsiyi.cpd/posts/131151736100567 (Accessed March 20, 2022)

34. DW. (2022, June 25). *Vitali Klitschko fake tricks Berlin mayor*. https://www.dw.com/en/vitali-klitschko-fake-tricks-berlin-mayor-in-video-call/a-62257289 (Accessed June 28, 2022)

35. President of Ukraine. (2022, August 22). *Elektronni petytsii. Ofitsiine internet-predstavnytstvo Prezydenta Ukrainy* [Electronic petitions. Official Internet representation of the President of Ukraine]. https://petition.president.gov.ua (Accessed August 22, 2022)

36. Ukraine. (1996). *Pro zvernennia hromadian* [On citizens' appeals]. Law of Ukraine № 393/96-VR. https://zakon.rada.gov.ua/laws/show/393/96-%D0%B2%D1%80#Text (Accessed August 22, 2022)

37. QHA / Krymski Novyny. (n.d.). *Media search results*. https://old.qha.com.ua/ru/search?t=%D0%BC%D0%B5%D0%B4-%D0%B8%D0%B0 (Accessed August 22, 2022)

38. European Commission. (2023, September 26). *Code of Practice on Disinformation: New reports available in the Transparency Centre*. https://digital-strategy.ec.europa.eu/en/news/code-practice-disinformation-new-reports-available-transparency-centre (Accessed September 26, 2023)

SECTION III

PRIVATE MILITARY COMPANIES – THE ASYMMETRICAL POTENTIAL OF MODERN ARMED CONFLICT

3.1. The Emergence and Development of Private Military Companies: Characteristics and Classification

PMCs have a long history, dating back to medieval mercenaries. However, the modern form of PMCs has become particularly widespread since the 1970s, when the first commercial military organizations began to appear, providing governments and private individuals with a wide range of military services. Ukrainian publications use various names for them, such as "private military companies" or "private war companies." Given the regulatory terminology used in Ukraine in the defense sector, the authors consider it appropriate to use the term "private military companies" [1]. Today, PMCs operate as integral parts of armed conflicts, leveraging unique opportunities to conduct operations in the modern military environment. Their influence is particularly noticeable in cases where states seek to achieve their goals while avoiding the direct involvement of regular armed forces.

PMCs play a vital role in modern armed conflicts and are increasingly acting as key players on the international stage [2]. Their emergence and growth can be explained by several factors, including geopolitical shifts, economic advantages, and the need to adapt to new types of conflicts and wars that occurred in the world at the end of the 20th century and continue into the 21st century. However, as their influence grows, questions of legal regulation arise that require additional attention from the international community.

These organizations provide a wide range of services, namely: reform and development of security and defense forces; planning

and preparation for their use; intelligence and counterintelligence; training of personnel; use, maintenance, and operation of weapons and military equipment; logistical support for security and defense forces; humanitarian demining; protection and direct participation in combat operations [3].

The rise of PMCs is a natural extension of the history of mercenaries who carried out military tasks for those willing to pay for their services. For centuries, mercenaries have been involved in conflicts, from medieval landsknechts to modern private armies. However, PMCs took their modern shape officially in the UK in the 1960s, with the first companies providing military services on a contract basis. The founder of the first modern-style Watchguard International, established in 1967, was British Army Colonel David Stirling. He had previously created the SAS (Special Air Service), a special military unit of the United Kingdom with the chief focus on reconnaissance and special operations, mainly in foreign countries [4]. The Control Risks Group was one of the first companies to offer security and safety solutions to governments and private companies. This approach gradually spread globally, and by the end of the 20th century, PMCs were actively involved in various conflicts and in protecting infrastructure in unstable regions.

The modern use of PMCs began at the end of the 20th century, following the collapse of the Soviet Union. After the Cold War ended, countries faced the need to participate in various regional conflicts, including peacekeeping, humanitarian, or purely military operations in high-intensity conflict zones, and many governments downsized their regular armed forces. PMCs became the ideal tool for such tasks: they provided a quick response, a high level of specialization, and no need for political justification to the public. The economic feasibility of using PMCs is another crucial factor in their development. The governments of many countries, including the US and the UK, faced the problem of high costs of maintaining regular armed forces, especially after the end of major military conflicts. PMCs became an attractive option for performing specific tasks, as their involvement allowed states to save on the costs of maintaining

large military units. In addition, many international corporations, especially in the oil and construction industries, began actively using the services of PMCs to protect their investments and infrastructure in conflict zones. For example, the protection of oil fields in countries such as Iraq and Nigeria is often carried out by private military companies. Modern wars, especially at the beginning of the 21st century, have become less formal, and conflicts have shifted to hybrid wars or low-intensity conflicts. In such conditions, PMCs have proven to be more effective than regular armed forces due to their flexibility, ability to quickly adapt to new conditions, and avoidance of public attention. War has become a business. The market for military services has grown, turning PMCs into key players in this business. For example, in 2009, the annual turnover of the private military services market reached $100 billion. This confirms that PMCs have become not only a strategic tool for governments and corporations, but also an important element of the global economy.

Another reason for the rapid spread of PMCs during this period was the increase in the number of "low-intensity conflicts" that required a flexible approach to warfare, particularly in Africa and the Middle East. Since these conflicts often did not require large regular armies, states and corporations increasingly turned to PMCs to carry out tasks in such areas.

One of the first examples of the successful use of PMCs was Executive Outcomes, established in South Africa in 1989 [3]. Its activities during the civil wars in Angola and Sierra Leone demonstrated the ability of small but well-equipped and professionally trained private military groups to accomplish tasks that regular armies often could not handle. This company set an example to follow and paved the way for the formation of an entire PMC industry.

This was followed by the creation of a number of other well-known companies, including Blackwater (founded in 1997 in the US), which became one of the world's best-known PMCs. Its role during US military operations in Iraq and Afghanistan was widely discussed in the international media. Blackwater, later known as Academi, now known as Constellis, has become a symbol not only of the

high professionalism of PMCs but also of the controversial situations associated with the use of private military units.

The functioning of PMCs in the international environment remains controversial from a legal perspective [2]. Although PMCs operate under contracts with governments or corporations, their legal status is often poorly regulated. Mercenary activities, which are prohibited by international conventions, do not fully apply to PMCs, as these companies have official status and operate within the legal framework of their countries. However, there is no single international legal framework governing PMCs' activities. Some countries have introduced domestic legislation to control the activities of PMCs, but the lack of global regulation leads to legal loopholes that allow PMCs to operate on the margins of legality. By comparison, the United States was the pioneer in legislating the activities of PMCs. The relevant regulatory document, FM 100-21, was adopted by the US Army Command in 1998 to regulate relations between the state and PMCs, namely between US Army personnel and PMC employees.

However, since the early 2000s, specialized services in logistics, security personnel training, security system development and implementation, and operations planning have been gaining popularity. PMC specialists have started to get involved in protecting production facilities, mineral deposits (mainly oil and gas), cargo escort, and other activities.

China, as one of the leading global geopolitical players, has also begun to actively use the potential of PMCs to protect its national interests. Although PMCs in China do not yet have the same popularity and influence as in the US or Russia, their role is growing in the context of international expansion and the protection of global projects such as the Belt and Road Initiative. Chinese PMCs operate not only within the country but also abroad, performing a wide range of tasks.

China, which had been a closed country for many years, experienced rapid economic development and the conquest of distant markets, coinciding with the fall of the Berlin Wall, the establishment of a new world order, the events of September 11, 2001, and the Arab revolutions. This acceleration of historical development prompted 10

million Chinese to move abroad to more than 200 countries [5]. Today, these Chinese abroad account for 37,000 Chinese businesses and manage $2 trillion in assets overseas [6]. The launch of the Belt and Road Initiative (BRI) in 2013, which is the largest geo-economic and geostrategic project of the 21st century, is directly linked to Beijing's activities in 70 countries, mainly in Central Asia, South Asia, East Africa, North Africa, and Eastern and Central Europe, as part of 900 structural projects worth $800 billion [7].

Ironically, between 2002 and 2019, 140,000 terrorist attacks affected countries in the BRI regions, resulting in 234,000 deaths [8]. According to the Chinese Ministry of Commerce, from 2010 to 2015, 345 terrorist incidents were linked to Chinese or Chinese companies abroad, resulting in over 1,000 deaths [9]. During this period, the Chinese government developed its foreign security doctrine in line with its economic and geostrategic ambitions. This resulted in outsourcing security for Chinese economic investments, privatizing security both domestically and abroad, and occasionally tempting the use of this discreet, globally scattered force for other purposes.

Until 1984, only four Chinese companies were allowed to operate abroad. All of them were linked to government institutions. In 1980, President Deng Xiaoping launched economic reforms and created four special economic zones on China's southeast coast. The first experiment covered the then-small cities of Shenzhen, Zhuhai, and Shantou in Guangdong Province, and Xiamen in Fujian Province. In 1984, the Chinese government decided to extend it to 14 major coastal cities, including Shanghai. That same year, the first Chinese company similar to a private security company (PSC) was established in Shenzhen, in one of the branches of the Public Security Bureau. In 1986, the Beijing General Security Company was founded, and it still operates today with 77,000 employees. Its activities are primarily centered on the domestic market in China. In 1994, Shandon Huawei Security Group was established, the first Chinese security company to operate abroad and accompany Chinese companies in their exports. It still exists today, mainly operating in Africa, where it provides protection for mining, oil, and infrastructure projects. A

year later, the China Security and Protection Group was established, which later became the main protector of the BRI.

In September 2009, the State Council of China issued the "Regulation on the Administration of Security and Guarding Services" (Baoan Fuwu Guanli Tiaoli). This measure was the government's first attempt to establish a regulatory framework for the private security industry and, de facto, to legalize PSCs. The regulations recognize two main categories of PSCs. First, "security companies" (baoan fuwu gongsi), which are tasked with training, security, and consulting on risk assessment and mitigation. Their personnel are equipped with non-lethal defensive weapons. Second, "security companies providing armed escort services" (congshi wuzhuang shouhu yayun fuwu de baoan fuwu gongsi). Such companies are allowed to equip their certified employees with combat weapons, but not with heavy military equipment or vehicles. This legal framework did not define the nature of these companies' activities abroad, but it allowed hundreds of small companies to open and larger ones to consolidate.

The launch of the BRI in 2013 revealed new challenges and completely changed China's foreign security paradigm. The emergence of mass terrorism after 9/11 plunged the Middle East into war, making oil companies vulnerable. 2004, a nightmare year for Chinese people abroad, marked a shift in people's perception of the duty to protect Chinese citizens abroad.

The influence of Chinese security companies varies widely and generally depends on states' willingness to protect Chinese citizens and on the resources at their disposal. Their work in this area will be more or less visible, depending on the country where they are located and whether local legislation allows foreigners to invest in security. For example, in Algeria, where this activity is strictly reserved for citizens, Chinese security companies operate by integrating with their clients or operating within consulting and logistics offices. Under the guise of managing the fleet and real estate of a Chinese company that needs to be protected, they control relations with local security authorities, escorts, convoys, protection of important facilities or in sensitive areas (on behalf of the end customer), and manage local security and protection partners [10].

In other regions of Africa, Chinese PSCs will operate as follows:

- Egypt, Tunisia, Algeria, Morocco: cooperation with local PSCs and government security forces to protect embassies, ports, and infrastructure, as well as respond to kidnapping for ransom (K&R). Training for Chinese clients is conducted in advance in mainland China. A notable aspect of Egypt is its maritime security against pirates.
- Libya, Sahel, and South Sudan: PSC activities are equivalent to those of PMCs, involving armed agents where possible. Such companies are typically used to guard mines and oil fields.

When the BRI was announced in 2013, it became clear that China would be sending millions of its citizens, billions of dollars, and thousands of companies to hundreds of countries where security was not always guaranteed. Erik Prince, founder of the American PMC Blackwater, saw this as a unique opportunity to significantly expand his business. He had the necessary knowledge, local connections, and a plan for military intervention to pacify countries in crisis by providing personnel and heavy equipment (armored vehicles, aircraft, boats, etc.) and a training program that could very quickly create a modern army. So, that same year, Prince joined forces with one of China's largest economic groups, CITIC, worth a trillion dollars, to create a private military company called Frontier Services Group (FSG) (Xianfeng Fuwu Jituan). Prince served as the chairman of the board of directors of FSG until 2021 (after which he was replaced by Israeli Dorian Barak, his financial advisor), and owned 25% of the company's shares. CITIC is a financial conglomerate owned by the Chinese government, so this is a real alliance between the Chinese government and Blackwater's founder. FSG was directly involved in the civil war in Libya on the side of Khalifa Haftar. Eric Prince, with funding from the Emirates, provided the Lebanese National Army with agricultural aircraft converted into bombers [11]. In 2019, he attempted to create a helicopter squadron and a "team of assassins," but failed [12]. Eric Prince and FSG chose Malta as their logistics and command platform for their operations in North Africa [13]. In China, in cooperation with the security services, he built a training center for security and urban guerrilla warfare in Xinjiang.

According to FSG, the agreement was signed at a ceremony on January 11, 2019, attended by Xinjiang officials and representatives of CITIC Guoan Construction. The agreement stipulates that FSG will invest $600,000 in the center, which will be able to train 8,000 people per year. In 2017, Eric Prince's Chinese subsidiary opened the International Security and Defense College in Beijing, which aimed to become "the largest private security training school in China" and train personnel for Chinese companies operating in Africa and Central Asia. In 2018, sources told Arabi21 that the security firm Frontier Services Group, headed by Erik Prince, who previously ran the security firm Blackwater, had recently sent fighters from the Kurdish region of Iraq to Libya to fight on Haftar's side, according to a secret agreement [14]. In addition to its activities in North Africa, FSG protects the interests of Chinese mining and oil companies in several regions of Africa, with personnel and logistics in Nigeria, Mozambique, and South Sudan.

Among the well-known Chinese PSCs are the following:

DeWe Security is one of the largest Chinese PSCs actively operating abroad. The company provides security for Chinese diplomatic missions, corporate facilities, and Belt and Road Initiative projects. DeWe Security is involved in the security of infrastructure projects in South and Southeast Asia, as well as in Africa, where China has significant economic interests.

China Security & Protection Group (CSPG), this company is one of the key players in China's PMC market. CSPG not only provides security for Chinese facilities abroad but also offers consulting and training services to local security forces. The company is active in Africa, particularly in Sudan and Nigeria, where China has strategically important investments in oil production.

Shandong Huawei Security Group – this company also specializes in providing security services for international Belt and Road Initiative-related projects. The company's main activities are concentrated in Africa and South Asia, where Chinese corporations need protection from armed groups and extremists.

In recent years, China has been increasingly engaging PMCs to assist with its international strategy, particularly in projects linked to the Belt and Road Initiative. This large-scale project involves the creation of infrastructure corridors connecting China with Europe, Africa, and other parts of the world, and ensuring their security is critical. Chinese PMCs enable the government to protect the country's interests abroad without involving the regular armed forces, allowing it to maintain diplomatic neutrality in many conflicts. This also allows China to remain an active participant in international politics while avoiding direct military intervention. China's PMCs continue to develop, and their role in global security is becoming increasingly prominent. Although they do not yet have the same combat capabilities as Western or Russian PMCs, their role in guarding and protecting infrastructure projects is an important element of China's strategy to expand its global influence.

Despite their rapid growth, Chinese military and security companies face many challenges [5]. The first of these is the low quality of security guard training, language barriers, and a lack of openness to other nationalities. At present, it is impossible (with the exception of FSG) to find a Chinese PMC with operational capabilities similar to those of Blackwater/Academi or Wagner Group. These capabilities require increased logistics and training, which Chinese companies currently lack.

The second challenge concerns staff salaries. They are too low, which does not contribute to the emergence of a world-class elite and does not encourage professionals in this field to join Chinese companies.

The third challenge pertains to Chinese legislation, which is poorly adapted to the global context of PMCs (their status is not recognized by law in China). Gun control laws are very restrictive, even for licensed companies (the PRC Firearms Control Law (Zhonghua Renmin Gongheguo Qiangzhi Guanli Fa), adopted in 1996, allows only the People's Liberation Army (PLA), police, and militia).

Finally, given the lack of a clear strategy, private military and security companies lack flexibility, obey only the orders of their

Chinese clients, and do not enter the international security market to benefit other companies or interests. As a result, Chinese PMCs are generally more restricted in the scope of their operational capabilities compared to their Western counterparts. They do not actively participate in combat operations but provide security for facilities and personnel, especially in high-risk areas. Given the high level of government control, Chinese PMCs focus on tasks that protect China's national interests abroad without involving the regular armed forces in conflicts.

The key areas of activity for Chinese PMCs are [5]:

- Protection of infrastructure facilities – China has substantial economic interests in Africa and Asia, and Chinese PMCs ensure the security of these projects. Specifically, they guard construction sites, transportation routes, oil and gas fields, and other vital facilities.
- Protection of personnel – Chinese companies and the government need to protect their personnel abroad, especially in countries where there is a threat of kidnapping or attack. Chinese PMCs provide security for employees of Chinese corporations, diplomats, and other state representatives.
- Consulting services and training – Some Chinese PMCs provide training services to local security forces, especially in countries where political instability poses a threat to Chinese projects. This also includes training in security methods, the use of modern security systems, and analytical work to assess risks.

As a result, China has developed PMCs at a slower pace and with stricter government oversight compared to other countries. This is due to China's traditional attitude toward private military organizations, which are often perceived as a potential threat to the state's monopoly on the use of force. The Chinese government has tight control over the security sector, and PMCs operating in China are strictly regulated to prevent unauthorized activities. Since the early 2000s, China has engaged PMCs to protect its facilities and infrastructure abroad, especially in Africa, where Chinese corporations have made large investments in natural resource extraction. The emergence of Chinese PMCs was a response to the need to protect China's economic interests in the

context of unstable political regimes in many countries. Chinese PMCs usually work in close contact with the government and state-owned corporations.

Although in Russia only the state has the official right to use armed forces, any other such activities are considered mercenary and are prohibited on Russian territory under threat of criminal punishment. Nonetheless, PMCs exist unofficially, positioning themselves on the Russian market as private security companies and providing a range of services only in the "European sector," where this is permitted. In the current environment, these organizations are highly effective, mobile, and versatile tools for carrying out certain governmental objectives [15].

One such objective carried out by Russian PMCs was the fighting in Georgia (2008), the military coup in Syria, the fighting in Ukraine, and many other military conflicts and wars. It is precisely the use of PMCs in war or armed conflict that allows a country, in particular the Russian Federation, to conceal its direct involvement, which was particularly evident in the Russian Federation's hybrid war against Ukraine and in the current stage of full-scale Russian-Ukrainian war.

Unfortunately, in the 21st century, the Russian Federation has taken the lead in the practical application of the concept of hybrid warfare involving PMCs. Armed aggression against Ukraine has created an ideal environment for deploying PMCs, as it allows for a variety of "operations" to be carried out without regard to, or even in defiance of, international humanitarian law, international conventions, and ceasefire agreements — from abusing prisoners to shelling residential areas. The Wagner PMC, founded by Yevgeny Prigozhin and named after its commander, Russian neo-Nazi Dmitry Utkin — "Wagner," chosen because of his fascination with the "aesthetics and ideology of the Third Reich" in honor of the German composer Richard Wagner [16].

In other words, it is evident that PMCs have become common worldwide, providing a range of services to various clients — including private individuals, governments, and international organizations.

Based on an analysis of the types of services provided by PMCs, relevant documents from international organizations, and publications, PMCs can be classified as follows [1, 17–19]:

1. *Defensive military companies*

The main function of defensive PMCs is to provide security for facilities and personnel, as well as logistics services and military training. These companies typically perform tasks related to the protection of critical infrastructure, including diplomatic missions, industrial enterprises, and oil and gas facilities. Defensive PMCs also provide training for local military and police forces and perform logistical support for military operations, including cargo transportation or medical support in conflict zones.

2. *Offensive military companies*

Offensive PMCs participate in combat operations and special missions. They execute tasks involving direct participation in wars and conflicts. This type of PMC is most often employed by states that do not wish to intervene openly in a conflict due to political or legal risks. The Wagner Group is a prime example of a combat PMC participating in various conflicts around the world, particularly in eastern Ukraine and the Middle East. These companies are often used to conduct covert operations or perform tasks that governments cannot carry out in the open.

3. *Intelligence and counterintelligence companies*

A distinctive feature of intelligence and counterintelligence PMCs is that they are ahead of special services in developing and utilizing the latest technologies in their operations, and their network functions as a effectively closed system. According to various online sources, American companies such as Strategic Forecasting Inc. and Booz Allen Hamilton, as well as British companies such as Aegis and Haklyut & Company, cooperate with state intelligence agencies. They can be used to conduct various forms of political competition, as well as not only to carry out orders from state bodies (including special services) and corporations, but also to acquire the status of an intelligence target for other countries seeking to obtain information possessed by private military companies.

4. *Hybrid military companies*

Hybrid PMCs perform both defensive and offensive tasks. They can provide logistics and security while conducting combat operations. This type of company is the most versatile and is used by both states and private companies to achieve their goals in unstable regions.

5. *Combat support companies*

PMCs that provide their clients with services to support the combat operations of their security and defense forces (in NATO terminology, tactical support), including direct participation in combat operations. However, the latter of these services is not provided by modern PMCs, at least officially.

6. *Military consulting companies*

PMCs specializing in providing services for the planning, creation, reform, and development of security and defense forces, including intelligence and counterintelligence agencies, their combat and special training, etc.

7. *Military logistics companies*

The scope of activities of these private military companies includes: maintenance and operation of complex weapons systems, military equipment, and computer systems; logistical support for troops; and construction of military facilities.

8. *Private security companies*

These include companies operating in conditions of military conflict or in high-risk areas, particularly in countries with unstable situations. Although they usually provide protection for facilities and individuals rather than engaging in combat operations, in areas of military conflict, there is no clear distinction between these types of activities. For example, when protecting airfields, oil pipelines, and other infrastructure, security companies may conduct combat operations against illegal military formations, terrorists, etc.

9. *Maritime military companies*

In recent years, PMCs have become actively involved in combating piracy, providing escort and armed protection for ships, negotiating with attackers, etc. Currently, there are more than 20 such

PMCs operating in the Gulf of Aden and the Horn of Africa alone. Shipping companies incur annual costs of approximately US$100 million to hire them [19]. Legal issues surrounding the activities of such PMCs were discussed in London in May 2012 at the 90th session of the Maritime Safety Committee of the International Maritime Organization. Among other things, the session approved a draft Interim Guidance for Private Maritime Security Companies providing private armed security services on ships in high-risk areas [20].

Thus, PMCs are a military-political phenomenon of the 21st century that poses a serious challenge to international law; they work for both government and private corporations. Since the establishment of Watchguard International, the first PMC in modern history, in the United Kingdom in 1967, there has been a steady trend towards growth in demand for such companies' services, an increase in the number of their customers, and an expansion of the range of services they offer. PMCs have taken a special place in the modern military-political sphere, strategies, and practices of states. This and many other facts indicate the direct interest of states in the existence of such companies and such businesses. At the present stage, it is extremely convenient for states, primarily Western ones, which are mainly the countries of origin of such companies, to use PMCs not only from an economic point of view, but also in order to preserve their political reputation. Currently, PMCs have become an integral tool in armed conflicts, which has led to various problems, ranging from human rights issues to the participation of militants in military operations and wars.

3.2. Capabilities of Private Military Companies in the Context of Destabilization of the International Security Environment

Non-state actors are playing an increasingly significant role in the hierarchy of key players in international cooperation, shaping the system of international relations and determining the main trends in its development. At the same time, their circle has expanded significantly and, by general consensus, now includes non-governmental

organizations (NGOs), international non-governmental organizations (INGOs), mass media, major political parties, transnational companies, international terrorist organizations, and others.

Non-state actors typically serve a dual role: they actively shape the broader patterns of international processes while also being subject to external influence and manipulation by traditional actors, mainly states, involved in global politics.

The practice of communicating with communities in other countries existed before. In particular, it was developed during the Cold War in both the USSR and the US. Even then, not only state bodies that dealt with public structures in other countries began to emerge, but also non-governmental entities in foreign countries. Examples include friendship societies with foreign countries in the USSR.

According to the traditional approach, non-state actors, in particular NGOs and INGOs, are seen as "interest groups" and "pressure groups" that are more likely to achieve results by changing government policies than by direct action. Thus, by influencing public opinion within a particular country, an INGO exerts pressure on the government of that country in the course of foreign policy decision-making.

In addition, states often engage INGOs to gather information and provide expert assessments. In exchange, INGOs expect to receive support from states, including informational support. The growing interdependence between states and INGOs is just one example of their interaction.

By providing information and mobilizing public opinion, INGOs are increasing their influence in the decision-making process within international intergovernmental organizations (IGOs) by sharing their perspectives on relevant issues. In recent years, the level of cooperation between IGOs and INGOs has steadily grown, enhancing INGOs' impact on international processes.

At the same time, the importance of the non-governmental sector in matters of national security needs to be seriously reconsidered. Even now, these entities do a great deal to help the state (both in the military domain and in many others, including information).

However, this cooperation remains based on the conservative attitude of state bodies towards any external players who, to one degree or another, seek to participate in the implementation of its functions. However, it should be recognized that the state can never be as highly mobile and flexible in its actions as non-state structures that are not constrained by formal bureaucratic rules and regulations.

Notably, Russia's use of its PMCs and other paramilitary structures (such as the Wagner Group and Cossack associations) on the territory of Ukraine has, to a certain extent, demonstrated the effectiveness of this model. The war in eastern Ukraine, which Russia started in 2014, was local in scope, but some Ukrainian politicians called it a hybrid war by Russia against Ukraine, in which the Wagner PMC was used as the main element of this war. It participated in the annexation of Crimea and later in hostilities in the Donetsk and Luhansk regions. This PMC can be called a classic example of mercenaries, an army of people convicted for serious criminal offenses, recruited from penal colonies and other places of imprisonment. During Russia's full-scale invasion of Ukraine, a significant part of the aggressor's military potential in this war was made up of PMC units (including the Wagner Group), whose activities are an example of modern mercenaryism and are aimed at overthrowing the government and the constitutional order.

Below, we will examine the capabilities of the most well-known PMCs and their involvement in various destabilization situations of the international security environment, including the Russian-Ukrainian war.

Blackwater (now known as Constellis). Blackwater became one of the most famous PMCs due to its activities during the wars in Iraq and Afghanistan. Founded in 1997, Blackwater specialized in providing security services, military training, and security for diplomatic missions. Its main goal was to support the US armed forces in conflicts after the terrorist attacks of September 11, 2001. The most well-known episode that attracted international attention took place in Baghdad. In 2006, a car accident happened in Baghdad's Green Zone. An SUV driven by Blackwater employees crashed into a US

Army Humvee. The Blackwater personnel disarmed the soldiers and forced them to lie on the ground at gunpoint until they drove their SUV away from the scene. On the evening of December 24, 2006, an employee of the company, intoxicated with alcohol, shot and killed the Vice President of Iraq's bodyguard, hitting him three times with a pistol. The mercenary who committed this act was dismissed from the company and deported from the country without any further sanctions.

A year later, in 2007, the American media suddenly began to report that Blackwater employees in Iraq were executing civilians. This primarily refers to an incident in which a convoy of armored vehicles carrying Blackwater employees was escorting cars belonging to US State Department officials. That day, Blackwater employees opened fire on civilians in Nisour Square. The incident resulted in the deaths of 17 and injuries to 20 civilians and caused an international scandal. The Federal Bureau of Investigation (FBI) immediately took up the case. Their conclusions were objective, as they say: the civilians were dead because they had also fired at the mercenaries.

However, the government did not side with Blackwater. Their contracts were revoked, four members were arrested, and they were stripped of their license to operate in Iraq. On the one hand, this was hardly a harsh punishment, but on the other, it meant tens of millions of dollars in losses. Their license was reinstated in late 2008. However, government agencies began to closely monitor Blackwater. All of their armored vehicles were required to be equipped with listening devices. Radio communications and correspondence between PMC members also became accessible to the special services. While the company stated that its employees responded to a threat, the incident increased criticism of PMCs and underscored issues with regulating their actions in conflict zones.

After the 2007 incident with civilians, the company fell on hard times. The blow to the agency's reputation was so severe that they had to completely reorganize their structure. In 2009, the company was renamed Xe Services LLC, and in 2011, it was renamed Academi. However, everyone still knows them as Blackwater. Erik Prince has

stepped down, and various special forces personnel have taken over management and control.

Blackwater also participated in military operations in Afghanistan, providing security and logistics services to the American military and diplomats. Despite criticism, the company continued operating under new names. In 2014, Academi merged with Triple Canopy, a subsidiary of the Constellis Group. Academi was later fully integrated into the parent company and now operates under the name Constellis, which provides security services under contract to the US federal government.

Blackwater has come a long way from being an ordinary security company to an elite unit of mercenaries ready to deploy to any hotspot on the planet. For them, there are no impossible tasks, taboos, or compassion — money decides everything.

DynCorp International. DynCorp is one of the largest American private military companies involved in numerous conflicts and peacekeeping operations. Its activities include providing logistical services, security, training local security forces, and humanitarian operations. One of DynCorp's main areas of activity is providing security for government facilities and diplomatic missions in countries such as Iraq and Afghanistan. In addition, the company actively cooperates with the UN and other international organizations in carrying out peacekeeping missions. DynCorp also provided security for Afghan President Hamid Karzai. DynCorp is known for its involvement in post-war stabilization processes, including the training of Iraqi police forces after the fall of Saddam Hussein's regime. It also provides support services to the US and other countries' armed forces, assisting with logistics and military training. However, DynCorp's activities have not always been without controversy. For example, in 1999, the company was involved in a peacekeeping operation in Bosnia and Herzegovina, where it was accused of involvement in human trafficking, which led to serious criticism at the international level.

Triple Canopy. Triple Canopy is one of the leading American PMCs, providing a wide range of military services, including security, training, and reconnaissance tasks. The company is actively in-

volved in conflicts in the Middle East, Africa, and Latin America. Triple Canopy provides security for diplomatic missions, government agencies, and private companies, particularly in Iraq and Afghanistan. Its role in conflicts involves not only security functions, but also support for intelligence operations, logistics, and consulting.

GardaWorld. GardaWorld is one of Canada's largest private military companies, providing security services and ensuring safety in various regions of the world, including dangerous conflict zones. The company specializes in protecting diplomatic missions, government institutions, and commercial facilities. One example of GardaWorld's activities is the protection of diplomatic missions and facilities in Afghanistan, Iraq, and Libya. The company also actively provides logistics services in conflict zones, ensuring the safe movement of goods and personnel through dangerous regions. GardaWorld is known for its effectiveness in providing security for private corporations operating in unstable regions, including oil and gas companies. It is also actively involved in humanitarian operations, providing support to international organizations and governments.

Aegis Defence Services. Aegis Defence Services is a British private military company founded in 2002 that specializes in providing security services, particularly in conflicts in the Middle East and Africa. Its main activities focus on providing security during peacekeeping missions and stabilization operations. Aegis Defence Services is known for its involvement in conflicts in Iraq, where it provided security and logistics for US and UK government agencies, as well as private companies. The company actively cooperates with governments and international organizations in ensuring security in dangerous regions.

Wagner PMC. In recent years, PMCs have been actively used in military conflicts involving the Russian Federation. However, their activities are illegal under current law, as exemplified by the Wagner PMC case. Wagner mercenaries served as the primary striking force, supplemented by airborne troops that had already suffered heavy losses and had their combat capabilities reduced substantially.

The Wagner PMC is a striking example of a modern Russian PMC involved in conflicts around the world, carrying out both official and unofficial orders from the Russian government. The Wagner PMC first appeared on the battlefield in 2014 during the annexation of Crimea and the war in eastern Ukraine, where its fighters supported pro-Russian forces. The Wagner PMC has become one of the key tools in Russian foreign policy, enabling the government to conduct military operations abroad while reserving the option for "credible denial." This enables Russia to avoid direct accountability for Wagner fighters' actions, which is a key aspect of hybrid warfare. One of the most notable episodes involving the Wagner PMC took place during the conflict in Syria, where it supported Bashar al-Assad's government. According to various sources, Wagner Group fighters took part in the battle for oil fields in the province of Deir ez-Zor in 2018. At that time, there was a clash between US-led coalition forces and Wagner Group militants, resulting in the deaths of dozens of Russian mercenaries. This episode confirmed that Wagner acts as an indirect instrument of Russia in conflicts in the Middle East. There are also reports of the Wagner Group's involvement in military operations in the Central African Republic, Libya, Sudan, and other African countries, where its troopers are involved in protecting governments and strategic facilities. This allows Russia to gain political and economic influence in the region, avoiding direct intervention with the regular units.

Thus, with the increase in the number of regional conflicts and global instability, the PMCs' role as instruments of warfare has grown significantly. They are capable of providing fast, flexible, and tailored solutions for military and geopolitical tasks in conditions where regular armed forces may be ineffective or unnecessary. Today, the demand for PMC services in modern military conflicts is growing rapidly. Multiple estimates suggest that the global market, valued at hundreds of billions of US dollars, is projected to nearly double over the next decade.

According to Global Growth Insights, the market for private military services (PMS) in 2024 was worth approximately $236.33

billion. It is projected to reach $254.15 billion in 2025, approximately $273.32 billion in 2026, and $488.9 billion by 2034. This steady growth reflects an average annual growth rate of 7.54% from 2025 to 2034 [21].

According to The Market Intelligence, the global private military services market was valued at $212.34 billion in 2024 and is expected to reach $221.69 billion in 2025, rising to US$312.86 billion by 2033, with an average annual growth rate of 4.4% during the forecast period [22].

Researchers at Custom Market Insights expect the market to record an average annual growth rate of 5.68% from 2025 to 2034 (Fig. 3.1). The market is projected to reach a value of $274.53 billion in 2025. By 2034, the market capitalization is expected to grow to $451.18 billion [23].

As provided, the current global PMC services market cap is estimated to be around $200–260 billion annually, with anticipated growth reaching $400–450 billion in the next decade. Additionally, industry experts at Custom Market Insights state that the adoption of new strategies and technologies by manufacturers creates lucrative

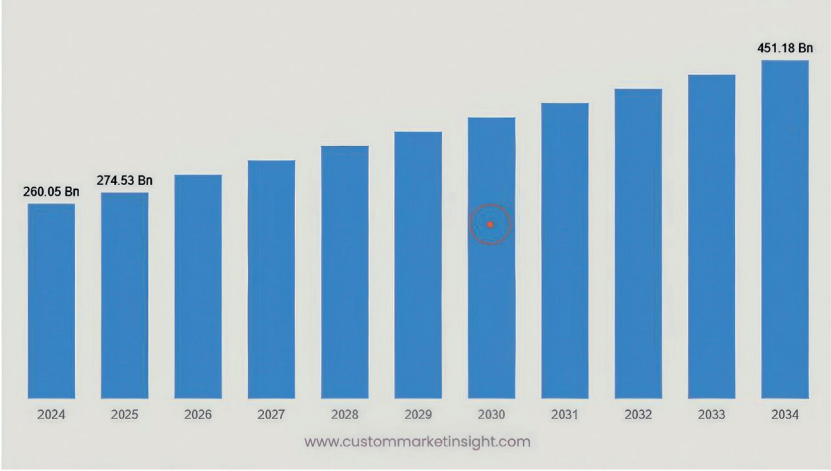

Fig. 3.1. Global private security services market from 2025 to 2034

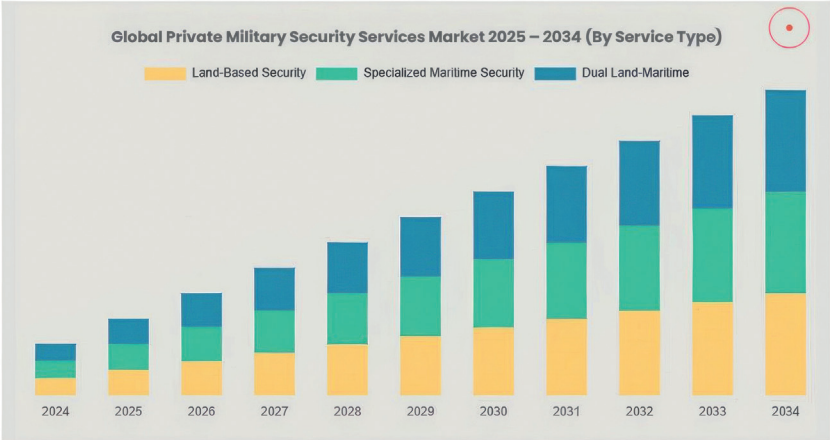

Fig. 3.2. Global private security services market (by type of service) for 2025–2034

opportunities for players in the private military security services market during the forecast period. (Fig. 3.2).

Experts highlight the following key trends and drivers of PMC development:

1. ***Growing demand for integrated security solutions.*** The growing demand for integrated security solutions, where physical and digital security are combined, is expected to drive market expansion. Customers want comprehensive services that include armed personnel, surveillance, risk analytics, and cyber protection all in one package. This approach ensures efficiency and lowers reliance on multiple service providers. Private security companies now offer hybrid models that blend traditional defense with AI-based monitoring, drones, and digital threat intelligence. As global threats become more complex and multifaceted, integrated solutions are increasingly necessary, with private security providers becoming essential partners in next-generation protection and risk management.

2. ***Increased use of cutting-edge technologies***. The latest technological developments have brought about significant changes in the private military and security services market. Companies are

implementing AI-based surveillance, biometric access control, predictive analytics, and drone surveillance to improve operational efficiency and threat detection. Robotics and autonomous systems are being considered solution for perimeter security and reconnaissance in high-risk areas. Cybersecurity is also becoming a critical component given the rise of hybrid warfare. Implementing advanced technologies lowers risks for PSCs, allowing them to deliver real-time intelligence and respond quickly to emerging threats. This trend makes companies more competitive and better prepared to meet the dynamic needs of businesses and governments.

3. ***The outsourcing of defense.*** Governments have begun outsourcing non-core defense functions to PMCs in order to save money and increase flexibility. Logistics, convoy security, building security, and threat analysis are common functions that have been outsourced so that official armed forces can focus on combat operations. This trend has gained momentum in countries participating in international missions or peacekeeping activities, where private companies play a vital supporting role. In addition to ensuring rapid deployment and access to specialized skills, outsourcing is also a cost-effective option. The growing use of PMCs to support defense functions generates a steady stream of orders, reinforcing the market's growth trend.

4. ***The growing need for critical infrastructure security.*** The security of critical infrastructure, such as oil fields, power plants, ports, and transportation networks, is a growing concern in the market. Critical infrastructure attracts attention from terrorists, pirates, and saboteurs in politically unstable or high-risk areas. Private military companies provide armed security, surveillance, and rapid response teams around the clock to safeguard these facilities. As investment in energy and infrastructure expands globally, the need for effective security solutions continues to grow. Companies increasingly rely on private providers for their quick deployment and flexibility in complex operating environments, ensuring the continuous operation of critical supply lines and national economic infrastructure.

5. ***Expansion into emerging markets.*** The expansion of private military security services is steadily growing in new regions, particular-

ly in Africa, the Middle East, and Southeast Asia. These regions suffer from persistent political instability, insurgencies, piracy, and underdeveloped state security institutions. Transnational mining, construction, and oil corporations rely on private security firms to protect their personnel and equipment. This creates opportunities for international players and new local entrants, fostering collaboration that combines global experience with local knowledge. This penetration into these regions will continue as long as instability persists and economic projects grow, leading to a significant expansion of private military corporations.

6. ***Growing focus on transparency and ethical standards***. The industry is now investing more in ethical behavior and transparency to address human rights violations and accountability. Scandals have forced PMCs to adopt stricter codes of conduct, improved training, and enhanced reporting. Some of these organizations are moving toward international harmonization and the creation of internal oversight mechanisms in an effort to gain the trust of governments, non-governmental organizations, and business clients. This focus not only helps companies win contracts in highly politicized markets but also enhances their reputations worldwide. Transparency and ethical practices as winning factors contribute to market expansion, ensuring long-term sustainability and customer trust.

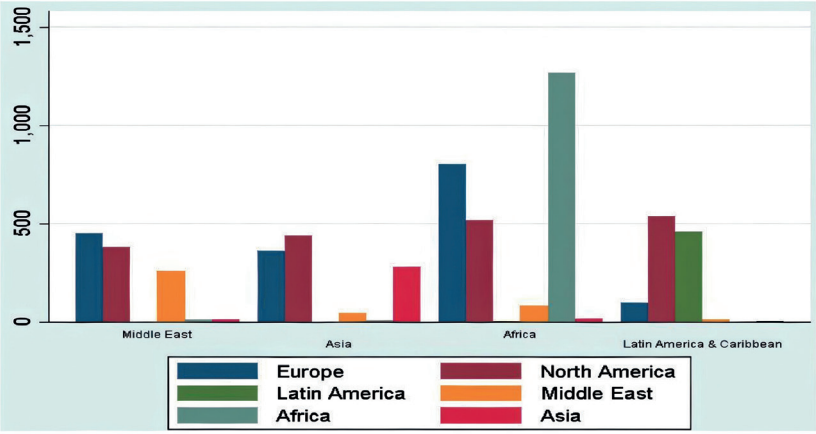

Fig. 3.3. Total number of PMCs operating in specific regions of the world

Figure 3.3 shows some striking trends in the distribution of countries where companies operating in different regions of the world are based.

First, the global power equipment market appears to be dominated by European and North American companies, which are the only ones operating in all regions. While North American companies have demonstrated similar levels of contracting activity in all regions, European companies have been most active in Africa, followed by the Middle East, Asia, and, to a much lesser extent, South America. Second, Asian, South American, and Middle Eastern companies, on the contrary, operated mainly in their home regions, while African companies' contracting activity in Africa was extremely high, only slightly less than the activity of all companies from all other regions combined [24].

The main advantage of using PMCs is that the authorities of different countries can use them to circumvent restrictions imposed by existing control mechanisms.

For example, the legislation limits the number of military personnel deployed abroad, but PMCs are not counted in that number. They can also be included in any operation as a unit adapted to perform specific (special, covert) functions. In many countries, PMCs are not required to provide information about their activities or their income. Their employees mainly work as consultants rather than military personnel. Another advantage for PMCs is that the local population does not harbor dissatisfaction, as they are not regular armed forces from a different country but rather multinational companies safeguarding vital facilities. In addition, this activity doesn't trigger domestic dissatisfaction, as no official casualties or losses among the armed forces would be reported, and the state will never pay compensation to the families of those killed in action. Another important argument in favor of PMCs is that they can operate in the so-called blind spot of all states' jurisdictions and carry out special (covert) operations. It is exactly this secrecy and the capacity to follow a hidden agenda that most states find appealing. The legislative framework governing the activities of PMCs is not fully developed, especially abroad,

which makes it impossible to control them. Only 35 countries have ratified the UN Convention against the Recruitment, Use, Financing, and Training of Mercenaries, and it remains largely unsuitable for countering new challenges. For the most part, the national legislation of individual countries also lacks effective mechanisms for holding mercenaries accountable for their crimes. Therefore, the denial of any links between PMCs and the state, national and departmental special services is a strong argument for their use.

Therefore, amid rising international tensions and the emergence of instability hotspots related to the migration crisis, political populism, and terrorism, the pursuit of national interests at any point on the map comes to the fore. PMCs are organizations that are common in global practice and are authorized by governments to carry out specific tasks.

Experts say that the history of using mercenaries to strengthen military capabilities goes back thousands of years, with the first mentions of them appearing well before the Common Era. Today, hiring people for military purposes is a lucrative business, and the practice of using such "commercial warriors" can be observed in many countries around the world. Interestingly, the most famous examples of the use of PMC services in combat zones are not even related to Russia, but to the United States.

According to O. Dakhno, the growth in popularity of PMCs began in the mid-1970s [25]. At that time, the first PMC contracts were signed with the US government. The first PMC in the US appeared in 1970.

Vinnell Corp signed a multimillion-dollar contract with the US government to provide specialized services for the training and establishment of a national guard in Saudi Arabia. Later, such organizations began to be created in African countries (South Africa) and Israel, and their numbers grew rapidly in the US and the UK. The large number of PMCs and their active operations led to the world's first congress of "mercenaries" (USA) in 1980.

In general, the period from the late 1980s to the early 1990s was also quite significant for the development of PMC activities. The end of the Cold War triggered a change in the geopolitical situation.

First, there was a trend toward reducing military funding, which led to a reduction in the number of soldiers, officers, and specialists in this field. Often, the only option for these people was to transfer to private companies.

Second, the same reduction affected government activities. It became more profitable for the state to engage PMCs to solve temporary geopolitical tasks than to maintain its own armed forces.

Third, the geopolitical situation on the world stage has changed. Spheres of influence have begun to be actively "redrawn," requiring the support of armed forces, and PMCs have become the ideal tool for this.

It is also worth noting that the United States made history as the first country to legislate the functioning of PMCs. The relevant regulatory document was adopted by the US Army Command in 1998 to govern relations between the state and PMCs, specifically between US Army personnel and PMC employees.

Another significant date in the history of PMCs is April 2001, when the first international organization regulating the activities of PMCs on the world stage, the Peace Operations Association (POA), was established. Since the 2000s, large international companies, corporations, and organizations have become interested in PMCs' services.

The primary factors that have driven the growing development of PMCs are:

1. The deepening problems of national security and defense support for some states, which are officially designated by the UN as "least developed countries" or regarded as "failed states." In the era of globalization, their governments frequently encounter challenges that are beyond their ability to address in many areas.

2. Many developing countries face the challenge of mastering new types of weapons and preparing their armies to counter current threats. The lack of specialists in these countries creates a need for certain types of assistance. To this end, corporations that manufacture weapons and the armed forces of developed countries are called upon, but most of this assistance is provided with the involvement of PMCs.

3. The reduction in the size of some countries' armed forces and the decrease in their state funding have pushed to a move toward outsourcing.

4. Growing demand for transnational corporations to secure their activities in unstable regions worldwide.

5. Increased demand for PMC services from international security and humanitarian organizations, especially for logistical support for peacekeeping operations, humanitarian demining, protection of humanitarian cargo, and more.

6. Economic aspects of PMCs' operations. The market for these services is marked by strong growth trends. During the first decade of the 21st century, it has transformed from a small specialized niche into a global sphere of military services.

7. Expansion of the supply of military specialists on the market, which allows PMCs to obtain highly professional personnel without investing in their training.

Since the beginning of the 21st century, PMCs have gained considerable popularity. The services of these organizations are utilized by both governments of many countries and international corporations. This market segment is developing quite actively and steadily. A real boom for PMC activities occurred when American troops invaded Iraq and Afghanistan. Many military experts claim that there are still a large number of "private soldiers" there.

PMCs also took an active part in the 2008 Georgian aggression, the military coup in Syria, military operations in Ukraine, and many other military conflicts.

Currently, there is a steady trend towards increasing demand for the services of such companies, with a growing number of customers and an expanding range of services. It is quite obvious that in contemporary military conflicts, PMCs function effectively as a type of special forces within the regular armed forces.

In general, PMCs are structures that perform special tasks in regions with complex military and political situations on behalf of the state. PMCs are capable of performing the following functions:

- Military protection of people and property, especially embassies or oil pipelines; safeguarding humanitarian missions.
- Participation in peacekeeping operations, including under the auspices of the UN.
- Mine clearance.
- Reconnaissance and assessment of the regional security situation.
- Maintenance and operations of combat systems and equipment.
- Combating piracy.
- Evacuation of the population from areas of armed conflict.
- Professional training of local police or military forces.
- Performing police duties in areas beyond the reach of law enforcement agencies.
- Detention and escort of detainees or prisoners.
- Training civilian staff to operate during emergency situations.
- Full participation in combat operations – jointly with regular units or separately.

PMCs also serve as a strong means for Russia to pursue its expansionist policies, either within the Commonwealth of Independent States (CIS) or in other parts of the world.

O. Ivasechko and T. Bondar argue that the first PMCs in Russia began to emerge almost immediately after the collapse of the Soviet Union. The reason for this was that after the collapse of the USSR, hundreds of thousands of former military personnel, KGB employees, police officers, etc., were left without work. It is unofficially believed that the first international conflict in which Russian PMCs were involved to secure national interests was the Transnistrian War [26].

However, the active period of PMC creation was 2014–2015, when Russia simultaneously began its intervention in Syria, annexed the Crimean peninsula, and occupied parts of the Donetsk and Luhansk regions. A distinctive feature of Russian PMCs is that they register themselves outside the domestic jurisdiction and have no official ties to the Russian Federation. This has enabled the Russian

authorities to use them as a covert tool for advancing geopolitical interests for nearly 10 years.

While in other countries, PMCs are separate commercial entities, in Russia, they are controlled by the ruling elite and are almost exclusively funded by the Russian Ministry of Defense. Therefore, it can be argued that Russian PMCs have become a hybrid form of PMCs, as they are not commercial entities independent of the state.

The Soviet Union once directed significant resources to the Middle East and Africa, which allowed it to maintain its influence and oppose the West and America. However, after 1991, the balance of power shifted, and with the collapse of the USSR, African and Middle Eastern countries began to lean toward a pro-European vector. By the early 2000s, the Russian authorities realized that they could lose this region and a significant part of their influence on the international stage with it, so they began gradually accommodating their foreign policy. According to the 2016 Russian Foreign Policy Concept, strengthening Russia's power, the competitiveness of its economy, and its international image are the main goals of its foreign policy.

In addition, in 2015, the Russian leadership approved the Russian Maritime Doctrine until 2020, which stated that the Mediterranean Sea was part of the strategy for regional maritime dominance and was one of the Russian Federation's meaningful foreign policy strategies.

The Russian authorities began their active engagement in Africa in 2010, and since 2014–2015, they have been engaging PMCs in regional conflicts. Russian PMCs have been spotted in Libya, Algeria, Sudan, Mali, Mauritania, the Central African Republic, Congo, Angola, Zimbabwe, Mozambique, Botswana, and Madagascar.

We can illustrate the activities of Russian PMCs by describing their role in Libya. Russian PMCs started operating in Libya's Second Civil War in 2015, with Wagner Group fighters being deployed there for the first time. Initially, Wagner Group fighters primarily focused on guarding strategic sites or training Libyan military forces. However, in 2019, a formal meeting took place involving the Libyan

army commander-in-chief, Khalifa Haftar, the Russian Defense Minister, Sergei Shoigu, and the Wagner Group leader, Yevgeny Prigozhin. During this meeting, they reached an agreement with Russia to allocate a military aid package and support Libya in the UN Security Council. In return, the Libyan authorities had to agree that the Wagner Group would control oil fields, two military bases, and a network of railways and motorways. This agreement allowed the Russian authorities to expand their influence in Africa and show their strength on the international stage.

The most painful and complex issue is the use of PMCs in Ukraine, as Russia used them to undermine territorial independence and wage a protracted war against the Ukrainian people. The most important goal of foreign policy towards the countries that were formerly part of the USSR is the desire to preserve its sphere of influence, dominate Russian interests in the policies of these states, and maintain economic control.

In his addresses to the Federal Assembly in 2003 and 2004, the Russian president stated that Russia considers the CIS space to be an area of strategic interest, while the 2008 Foreign Policy Concept defines a so-called boundary where the intersection of Russian, US, and European interests will be considered a threat to national security. Ukraine is mentioned as it has a favorable geopolitical location, and control over this territory would allow Russia to influence the West, gain complete control of the Black Sea, and increase its influence on the international stage.

Ultimately, losing Ukraine would mean a significant power loss for the Russian Federation and a complete failure of its imperial policy. When using private military companies during the annexation of Crimea and the occupation of the Luhansk and Donetsk regions, Russia set the following goals:

- Make Ukraine's accession to NATO and the EU impossible.
- Create new points of influence on the Ukrainian government and Europe.
- Minimize the possibility of Ukraine becoming a regional leader.

- Exhaust the Ukrainian economy by waging war.
- Block a significant part of the trade routes that were important for the existence of the country as a whole.

In fact, these actions confirmed that Russia's foreign policy had shifted back to imperialism. Interestingly, Ukraine was labeled as an unfriendly state in the 2016 Russia's Foreign Policy Concept, but it is not mentioned in the updated 2023 Concept.

Thus, today, PMCs have become widespread throughout the world. They perform a wide variety of services for various clients, which can be both private individuals and states. Most PMCs are registered in Western countries. At the same time, they operate in different regions of the world. Mainly in areas of conflict: the Middle East, Africa, Latin America, and others.

Foreign experience demonstrates that the scope of PMCs' activities across various regions is quite extensive. They are tasked with building military infrastructure, protecting cargo and diplomatic facilities, training and educating military personnel, introducing military technologies and producing weapons, conducting reconnaissance or counterintelligence operations, as well as participating in combat and counterterrorism efforts. Additionally, they take on certain sensitive tasks where law enforcement agencies and the armed forces cannot be officially involved.

3.3. Features of Intelligence Activities by Private Military Companies

Some large PMCs have specialized intelligence units that conduct professional intelligence operations for governments or corporations. These units are highly trained and utilize modern equipment to gather information. They also coordinate their activities with national intelligence agencies.

The intelligence efforts of PMCs are a crucial part of their operations in conflict zones. PMCs have the ability to carry out both strategic and tactical intelligence tasks, giving them an advantage in

quickly collecting information about the enemy or operational conditions. These capabilities are actively employed both on the battlefield and in information warfare.

The intelligence activities of PMCs may include gathering and analyzing information necessary to ensure security and complete their contracts. These activities can involve both overt and covert data collection methods aimed at identifying threats, evaluating the situation, and providing intelligence to support PMC operations.

A key feature is that PMCs have greater flexibility than regular armies in their methods of gathering intelligence, making them very useful for covert operations and hybrid warfare. Companies such as Wagner PMC often carry out complex intelligence tasks in high-risk environments, employing non-linear warfare methods, including electronic warfare, open-source analysis, and infiltration of agents into enemy structures [16]. Let's examine the main areas of PMC intelligence activities.

Tactical reconnaissance. PMCs are frequently involved in collecting tactical intelligence directly during combat operations in conflict areas. This may include:

- Gathering information about the enemy's location, weapons, logistics, and communications.
- Analyzing the terrain, climate, and infrastructure for planning.
- Assessing threats to personnel and protected sites, including potential attacks or sabotage.

For example, PMCs operating in conflict zones like Afghanistan or Iraq gather information about terrorist groups, their routes, and attack methods. This helps them secure facilities and plan actions to reduce risks.

Strategic intelligence. Besides executing tactical tasks, PMCs also engage in strategic intelligence gathering. This involves long-term monitoring of the political and military landscape in the region. PMCs analyze regional security, political risks, and economic conditions to help clients make informed decisions. For example, PMCs operating in Africa, where China or Russia have strategic econom-

ic interests, often collect information on the political landscape, the sentiment of local residents, and the activities of other actors, including insurgents or rival states [16].

Counterintelligence activities. As part of safeguarding facilities and personnel, PMCs also conduct counterintelligence measures to prevent the infiltration of enemy agents or saboteurs. This may include:

- Detection of espionage activities and monitoring of communications.
- Gathering information about possible sabotage groups and their plans regarding PMC's facilities.
- Protection against cyber threats and attempts to penetrate internal security systems.

Open source intelligence, OSINT. Modern private military companies widely use methods of gathering information from open sources, including the Internet, social media, news platforms, and specialized analytical publications. This allows them to quickly obtain information about events in their region, monitor changes in the behavior of various groups, including terrorist or insurgent groups, and predict possible threats to their clients. For example, the Wagner PMC actively uses OSINT to gather information about political sentiments in African and Middle Eastern countries where they operate [16]. This helps analyze potential threats to Russian interests and plan further operations with an eye toward the risks.

Technical intelligence and electronic warfare.

Many PMCs have technological means for signals intelligence (SIGINT) in their arsenal, including monitoring enemy radio communications, intercepting data, and conducting electronic warfare. This allows them to obtain important information about the enemy's plans or location, as well as disrupt communications between enemy units. For example, during operations in Syria, the Wagner Group used electronic means to monitor communication lines between opposition groups [16]. This enabled them to gather information about enemy plans and effectively disrupt their coordination.

PMCs may conduct intelligence gathering to protect their interests, ensure the safety of personnel and facilities, and support their operations. They use various methods of intelligence collection, including open sources, observation, analysis of open data, and covert methods, if permitted by law and contract terms. The primary methods and tools of PMC intelligence operations include:

- *Agent operations.* One traditional method of gathering information is through agents operating in the field. PMCs may use local populations, former military personnel, or politically interested individuals to obtain internal information about enemy plans, structure, supplies, and other important aspects. Agents may work undercover or disguised as civilians to reduce the risk of exposure.
- *UAVs and drones*. Modern PMCs are increasingly using UAVs to gather intelligence. Drones allow reconnaissance to be conducted over large areas without involving ground units and reducing the risk to PMC personnel. They are used to monitor territory, gather visual information, and detect enemy movements. For example, PMCs operating in Africa often use drones to monitor transport routes and ensure the safety of convoys carrying valuable cargo such as oil or minerals.
- *Social media analysis and intelligence gathering*. Private military companies also actively use information technology to monitor social media, where data on enemy intentions, attack plans, or changes in the political situation may be available. Intelligence gathering allows them to track not only local events but also global trends that may affect the security region.

Therefore, PMCs are effective at conducting reconnaissance across various areas, such as political, economic, and military, depending on their clients' needs and the specifics of their contracts. The intelligence activities of PMCs differ from those of state intelligence services in that they are limited by the tasks set by the PMCs and the terms of their contracts. The intelligence activities of PMCs may be regulated by national and international legislation on private military activities and information gathering.

Conclusions to Section III

This section examines PMCs and their use and role in modern armed conflicts. It considers the reasons for the emergence of PMCs, their history, and development. It analyzes the specifics, features, and areas of activity of the most well-known PMCs in the UK, the US, China, and Russia. It shows that PMCs can provide states and private individuals with a wide range of military services. It demonstrates that today PMCs function as an integral part of armed conflicts, utilizing unique opportunities to conduct operations in the modern military environment, where states seek to achieve their goals while avoiding direct involvement of regular armed forces. Based on the analysis of the types of services provided by PMCs, relevant documents from international organizations, and publications, they can be categorized as: defensive military companies; offensive military companies; intelligence and counterintelligence companies; hybrid military companies; combat support companies; military consulting companies; military logistics companies; PSCs; and maritime military companies.

References

1. Horovenko, V., & Tiutiunnyk, V. (2013). Pryvatni voienni kompanii: mizhnarodnyi dosvid i mozhlyvi shliakhy yoho realizatsii v Ukraini [Private military companies: international experience and possible ways of its implementation in Ukraine]. *Nauka i oborona*, (3), 32–39.

2. Semeniuk, Yu. V., Mokliak, S. P., & Lysetskyi, Yu. M. (2021). *Rozviduvalna diialnist i mizhnarodni vidnosyny. Novi realii ta pidkhody: monohrafiia* [Intelligence activity and international relations. New realities and approaches: monograph] (Yu. M. Lysetskyi, Ed.). LAT&K.

3. Avtushenko, I. B., & Avtushenko, O. S. (2024). Pryvatni viiskovi kompanii yak odyn iz instrumentiv vedennia suchasnykh viin [Private military companies as a tool of waging modern wars]. *Viiskovo-naukovyi visnyk*, (41), 120–132.

4. Wikipedia. (2025). *Pryvatna viiskova kompaniia* [Private military company]. https://uk.wikipedia.org/wiki/Приватна_військова_компанія (Accessed May 4, 2025)

5. Kharief, A. (2022, March). *China's discreet game in North Africa – Private military companies*. Rosa Luxemburg Stiftung. https://rosaluxna.org/publications/chinas-discreet-game-in-north-africa-private-military-companies/ (Accessed June 7, 2025)

6. Bartlett, D. (1997). *The political economy of dual transformations: Market reform and democratization in Hungary*. University of Michigan Press.

7. Chatzky, A., & McBride, J. (2019, February 21). *China's massive Belt and Road Initiative*. Council on Foreign Relations. https://www.cfr.org/backgrounder/chinas-massive-belt-and-road-initiative (Accessed June 7, 2025)

8. Institute for Economics & Peace. (2020). *Global Terrorism Index 2020: Measuring the Impact of Terrorism*. Sydney, Australia: Institute for Economics & Peace. http://visionofhumanity.org/reports (Accessed February 23, 2026)

9. Yuan, J. (2022). China's private security companies and the protection of Chinese economic interests abroad. *Small Wars & Insurgencies*, *33*(1–2), 173–195. https://doi.org/10.1080/09592318.2021.1940646

10. Glassdoor. (2025). *Security Officer Interview questions in Oran*. https://www.glassdoor.co.in/Interview/department-d-oran-security-officer-interview-questions-SRCH_IL.0,18_IS3581_KO19,35.htm (Accessed June 7, 2025)

11. Delalande, A. (2017, January 14). *Erik Prince's mercenaries are bombing Libya*. Medium. https://medium.com/war-is-boring/erik-princes-mercenaries-are-bombing-libya-88fcb8e55292 (Accessed June 7, 2025)

12. Kharief, A. (2020, May 15). Des mercenaires occidentaux ont aidé Haftar dans son offensive contre Tripoli en 2019 [Western mercenaries helped Haftar in his offensive against Tripoli in 2019]. *Middle East Eye*. https://www.middleeasteye.net/fr/actu-et-enquetes/libye-haftar-mercenaires-occidentaux-emirats-prince (Accessed June 7, 2025)

13. GlobeNewswire. (2014, November 17). *Frontier Services Group sets up operations in Malta*. https://www.globenewswire.com/news-release/2014/11/17/1236402/0/en/Frontier-Services-Group-Sets-Up-Operations-in-Malta.html (Accessed June 7, 2025)

14. North Africa Post. (2019, April 30). *Libya: Foreign mercenaries recruited for Haftar by security company*. https://northafricapost.com/30417-libya-foreign-mercenaries-recruited-for-haftar-by-security-company.html (Accessed June 7, 2025)

15. Skibitskyi, V. (2020, June 17). *Pryvatni viiskovi kompanii ta yikh rol u suchasnykh rehionalnykh konfliktakh* [Private military companies and their role in modern regional conflicts]. Speech at the 949th OSCE Forum for Security Cooperation. https://vienna.mfa.gov.ua/en/news/ (Accessed May 28, 2025)

16. Sliusarenko, A. V., Furman, I. I., & Pecheniuk, I. S. (2023). *Pryvatna viiskova kompaniia «Vahner»: vid stvorennia do sohodennia: monohrafiia* [Private military company "Wagner": from creation to the present: monograph] (M. V. Koval, Ed.). Kyiv, Ukraine: National Defense University of Ukraine.

17. Uesseler, R. (2008). *Servants of war: Private military corporations and the profit of conflict. New York, NY*: Soft Skull Press.

18. Valetskiy, O. (2006). *Chastnyye voyennyye kompanii, ikh sozdaniye, razvitiye i opyt raboty v Irake i drugikh regionakh mira* [Private military companies, their creation, development and work experience in Iraq and other regions of the world]. http://www.vrazvedka.ru/main/analytical/valeckiy.html (Accessed May 4, 2025)

19. IR-INGR. (2025). *Nebolshaya statistika po morskim ChVK* [Small statistics on maritime PMCs]. http://ir-ingr.livejournal.com/883373.html (Accessed May 4, 2025)

20. Advis.ru. (2012, May 31). *Informatsionnoye agentstvo INFOLine* [Information agency INFOLine]. http://www.advis.ru/php/view_news.php?id=3E9550FB-EADD-5840-901F-0023FFEB14E1 (Accessed May 4, 2025)

21. Global Growth Insights. (2025). *Private military services market size, share, growth, and industry analysis*. https://www.

globalgrowthinsights.com/enquiry/request-sample-pdf/private-military-services-market-104457 (Accessed August 6, 2025)

22. The Market Intelligence. (2025). *Private military services market size, share, growth, and industry analysis*. https://www.themarketintelligence.com/market-reports/private-military-services-market-1809 (Accessed August 6, 2025)

23. Custom Market Insights. (2025, September 10). *Global private military security services market size is expected to reach USD 450.1 billion by 2033* [Press release]. https://www.custommarketinsights.com/press-releases/private-military-security-services-market-size/ (Accessed August 6, 2025)

24. Petersohn, U., Gottwick, V., Penel, C., & Kellgren-Parker, L. (2022). The Commercial Military Actor Database. *Journal of Conflict Resolution*, *66*(4-5), 899-923. https://doi.org/10.1177/00220027211072528

25. Dakhno, O. (2020). Svitovyi dosvid stvorennia ta rozvytku pryvatnykh viiskovykh kompanii yak instrumenta realizatsii natsionalnykh interesiv [World experience in the creation and development of private military companies as a tool for the realization of national interests]. *Filosofiia ta politolohiia v konteksti suchasnoi kultury*, *12*(2), 61–68. https://doi.org/10.15421/352035

26. Ivasechko, O., & Bondar, T. (2024). *Pryvatni viiskovi kompanii u zovnishnii polititsi rosii: 2014–2023 roky* [Private military companies in Russian foreign policy: 2014–2023]. *Humanitarni vizii, 10(1),* 1–6. https://doi.org/10.23939/shv2024.01.001

SECTION IV

TRANSFORMATION OF INTERNATIONAL RELATIONS AS A FACTOR INFLUENCING INTELLIGENCE ACTIVITIES

4.1. National Interests as the Motivational Basis for the Activities of Intelligence Agencies

Goal-oriented human activity is based on needs and interests determined by certain personality traits that depend on the surrounding environment: material, social, and spiritual.

Needs and interests are not interchangeable concepts. Needs express the attitude of any active subject toward the necessary conditions of their existence, since without the satisfaction of a number of basic needs, neither biological nor social organisms can exist. However, not every need can fully stimulate a particular type of activity. A need, expressing the relationship between the subject and the conditions of its vital activity, manifests itself in unconscious desires and quite conscious motives for behavior. The true cause and driving force of social development is interest. Interests are conscious needs shaped by society, social groups, and individuals.

In 1935, the term "national interests" was first introduced into the Oxford Encyclopedia of Social Sciences. Since then, research on this issue has remained as relevant as ever, as it is one of the foundations for the conceptual development of the problem of democracy.

In English-language literature, this concept is used to mean "state interest." National interests are understood primarily as the interests of the state, since Western countries are mono-national states in socio-political terms. The nation represents the unity of civil society and the state, so the national interest becomes a general interest that removes the contradiction between the interests of the state and civil society.

In democratic countries, the national interest is, first and foremost, the interest of the people who form the political nation, generalized in accordance with existing procedures. The formation of the national interest involves the coordination of the interests of all citizens of the country, although sometimes this boils down to taking into account the opinions of the most numerous social groups.

V. Smolianiuk emphasizes that of the two main approaches to the nation (political and ethnic), in this case, the choice falls on the political nation as a political community of citizens of a particular state, as "a group of citizens who pursue collective and national interests through the mechanism of their own political organization — the nation state" [1]. The nation is defined as the main state-building element, the bearer of state sovereignty, the source of state power, and national interests. We would add that it is also the starting point for defining national security.

National interests are a consequence of the nation's "attitude towards its own needs in terms of domestic and foreign policy, which causes negative or positive conditioning of its activities, active choice of development paths, and turns into motives and incentives for historical creativity" [2]. These interests are formed on the basis of a system of national needs, which, in turn, are determined by the social (national) necessity to create a state, protect sovereignty, develop the economy, political system, legal system, morality, maintain an appropriate standard of living for the population, etc.

The legislative definition of the term "national interests of Ukraine" was announced in 2003 [3]. At the same time, the authorities have not proposed a normative legal act that would provide an exhaustive list of national interests throughout the entire period of Ukraine's national and political independence. As a rule, government documents are limited to "priorities of national interests," "vital national interests," "priority national interests," and "fundamental national interests." Such diversity significantly broadens the scope for explaining national interests, but deprives them of the clarity of verbal articulation that is necessary in this case. The situation was described at the time by M. Mykhalchenko: national

interests in Ukraine are still developing and therefore do not constitute a balanced system.

In the domestic context, there is acute ideological, political, and economic confrontation between various social forces, political parties, and socio-political leaders over the hierarchy of national interests, their content, and mechanisms for implementation [2]. Externally, it is impossible to ignore the European choice of the Ukrainian nation and the active opposition of the Russian Federation in this regard, which manifested itself in the occupation of part of Ukraine's territory (the Autonomous Republic of Crimea and the city of Sevastopol) in 2014, the outbreak of military aggression in the east of our country, and, after February 24, 2022, in the large-scale invasion of Ukraine. These and other factors increase the complexity of formulating universally accepted national interests that would be supported by all categories of the population throughout Ukraine. We have to limit ourselves to "framework" principles for defining national interests, which have both supporters and critics. Even more complicated is the situation with defining national values, which are not represented in national legislation as a separate regulatory and legal development. Some authors include religiosity, multi-confessionalism, multi-ethnicity, multiculturalism, family values, territorial integrity, the natural environment, scientific, educational, and scientific-technical potential, state sovereignty, the cultural and material achievements of the people (in particular, economic potential), democratic institutions as a prerequisite for ensuring the equality of the peoples inhabiting Ukraine, progressive socio-political development, as well as defining features of the national character (freedom-loving, hard-working, tolerant, friendly, peace-loving, self-sacrificing in defending the homeland, acute sense of social justice, democracy, tendency to preserve traditions) [4]. As a result of the extrapolation of national values to the specific historical conditions of the nation's development, corresponding national interests are formed. The highest-priority ones (vital, fundamental), as mentioned above, are declared at the official (state) level.

Challenges, threats, and dangers pose destructive influences on national interests and activities to protect them; in Western political culture, these are mostly grouped under the term "risks." Almost always, unforeseen influences (risks) on the national security system should be expected and can be described as "uncertainty" [5].

The phenomenon of uncertainty is confirmed by the political experience of most modern countries. Let us consider various manifestations of uncertainty that directly or indirectly affect national security.

Uncertainty 1. Since its principles were first articulated publicly in the early 20th century, national security has traditionally been perceived as a condition in which the vital interests of individuals, society, and the state are protected, ensuring their steady development and minimizing adverse risks. Almost always, "vital interests" were variably represented as "national interests" fueled by "national values." Both national interests and national values were enshrined in law in the pages of relevant regulatory and legal developments — laws, strategies, and doctrines. The category of "nation" seemed unquestionable as the starting point for articulating national interests and values.

Recent socio-political transformations have called into question the nation's supremacy within the overall spectrum of social relations. Nations are not fixed elements of sociogenesis, their static features change, evolve, and sometimes cease to exist. The intensification of migration flows, including migrant workers, refugees, and asylum seekers, calls into question the exclusive position of nations as established units of socio-political analysis, which was characteristic of the last century. Political, ethnic, and cultural theories of the origin of nations are becoming only "partially valid," failing to reflect the full range of social dynamics. Quite often, an individual's formal residence in a particular country does not in any way confirm their full membership in the local nation. Individuals may not accept (reject) the interests and values of their new social environment, which (from the point of view of the formal leaders of the host country) are defined as national. The fundamental pillars of national security are

being eroded, and our hypothetical migrant is in no way prepared to defend them.

This creates a contradictory situation: on the territory of a particular nation-state, which has proven its stability in previous historical tribulations, there are now increasingly more individuals (social groups) who do not feel a full sense of belonging to their "new homeland" and its sphere of national security. In quantitative terms, such groups are constantly growing, relying on their own sociocultural, linguistic, religious, everyday, and other characteristics. As a result, in the socio-political realities of our hypothetical country, we have national security that is "not for everyone." It does not accommodate the numerous variations in the individual (family, clan) lifestyles of migrants, which do not align with or at times contradict the state's approaches to ensuring national security.

Uncertainty 2. It is evident from the ruling elites' insufficient readiness to regulate national security on the basis of a "domain" approach. In Ukraine, legislative provisions have previously been made to ensure national security in established domains – political (domestic and foreign), economic, social, military, information, technological, spiritual and cultural, environmental, humanitarian, state border security, civil protection of the population, etc. The latest additions to the list of areas of national security are cyber and migration security, whose importance in today's conflictual relations is constantly growing. Despite lawmakers' efforts to prescribe the maximum number of areas on the pages of a particular state document, there remained social niches (areas) that did not fall within the defined list. These included, in particular, religious, maritime, ethno-national, and food security areas.

Thus, the "domain" differentiation of the phenomenon of national security does not account for the diversity of social life or the need for its multilateral monitoring. In modern conditions, any fragment of physical, cybernetic, or spiritual space where human activity is present can become an environment for the emergence of various threats and state and social countermeasures against them. Accordingly, although a narrow interpretation of dangerous situations

in areas defined by law is applied in practice, it is giving way to a comprehensive view of diverse threatening influences that can manifest themselves in a wide range and undermine the pre-established "domain" security construct.

Uncertainty 3. It can be seen in the differing interpretations of the nature of impulses directed against it. To specify such influences, some countries (particularly post-Soviet ones) widely use the terms "challenges," "threats," and "dangers." It is believed that their main difference is the intensity of the destructive impact on national security: a challenge can lead to its partial deformation, a threat to damage, and a danger to complete destruction without the possibility of subsequent recovery. However, national legal systems do not provide a comprehensive explanation of these terms. In security realities, these terms are arbitrarily mixed. In particular, the degradation of the security environment is described by various authors through arbitrarily constructed juxtapositions: challenge versus danger, threat versus challenge, threat versus danger, etc. Such verbal constructs further cloud the understanding of national security and reinforce the undefined (irrational) component of its evolution. In national security activities, such verbal indiscipline creates additional conditions for its subjective understanding and practical implementation.

To remedy the situation, the Western term "risk" has recently been used more widely as a universal semantic equivalent of challenges, threats, and dangers. This helps to define the security situation more adequately, but it also broadens the scope of subjectivity in security diagnostics.

Uncertainty 4. In terms of national security instruments, there is excessive subjectivity in determining the structure, functional purpose, and resource provision of the security and defense sector, the main instrument for carrying out national security activities in social segments where physical (armed force) activity remains dominant.

In the most concise terms, the security and defense sector can be described as "all law enforcement agencies" created by a democratic state and focused on securing national interests. First and foremost, this refers to the armed forces (army), police, national guard, peni-

tentiary authorities, security services, border protection, emergency services, intelligence agencies and their control centers, and some other special-purpose state bodies. Some countries add military-industrial complex and civic associations that deal with security and defense issues to this list.

This results in a rather complex format of state and non-governmental entities aimed at ensuring national security. At the same time, the ruling political elite single-handedly determines the "safety margin" of the security and defense sector, which depends on the number of armed formations (services) assigned to it and the methods of their training and deployment. The requirements for unifying the security and defense sector in politically integrated countries (e.g., NATO) are rather vague. Each country that is a member of the Alliance is capable of exercising "security and organizational creativity" to establish security institutions that, in the state's opinion, are most appropriate for the current risks. As a result, the process of establishing cooperation between the security and defense sectors of different states becomes more complicated, as the formal similarity of the security forces of different countries is blurred by the specifics of national thinking on security and defense issues and national reservations about the necessity/unnecessity of including a particular body in the national security system.

The situation is complicated by the enduring sympathy of autocratic systems for the state military organization (SMO) – the counterpart of the security and defense sector in democratic countries. According to the Russian leadership, the ideology of SMO dominance in political relations within the country and beyond its borders is supported by states that sympathize with the Russian regime. The fundamental difference between the security and defense sectors and the military organizations of states lies in the presence/absence of comprehensive democratic control over the security forces and the impossibility of a single state leader using the state's security resources. In democratic countries, such control is a given, a sign of a nation's security and defense culture. In contrast, in autocratic states, democratic control is either a formality or absent altogether. This

creates additional social uncertainty: how is it possible to establish interaction (let alone cooperation) between the security and defense sectors and state military organizations, which by their very nature were and remain civilizational antitheses? This happened once (in the exceptional military-political conditions of World War II, when the anti-Hitler coalition of states was forged). The next 80 years of world history, dominated by the Cold War between the geostrategic West and East, proved that it was impossible to recreate such a format of interstate relations. In today's world, social uncertainty as a factor influencing security and defense policy is exacerbated by the political impossibility of British-Russian, American-Chinese, or Belarusian-Polish cooperation in the field of strengthening international security through the formation and practical application of mixed military contingents.

Uncertainty 5. In the context of nonstate support for security and defense policies, a separate issue is the inability to ascertain in advance the *optimum* of the state-citizen interaction on issues of national security in times of peace and war. Social experience has repeatedly demonstrated the ability of interested communities to decisively influence political power – to correct the state's course, change the political regime, and achieve personal changes in the ruling elite. However, state-citizen interaction becomes particularly sensitive during military conflicts (wars). Here, two scenarios may unfold.

If the legitimate authorities appeal to the need for armed protection of national interests and values, there will be a pro-state polarization of patriotic civil society groups with the aim of providing comprehensive assistance to the authorities. Society acts as a resource for the stability of the state. On its own accord, under force majeure circumstances, self-defense forces, volunteer battalions, and territorial defense units and divisions rapidly emerge to defend the state alongside the armed forces. Other important manifestations of the community's security (defensive) activity include volunteer movements, think tanks, and media organizations, whose significance has been and remains extremely important. This is how the potential for national stability and society's ability to self-organize manifests itself.

In the event of the elimination (destruction) of the state by an enemy, the community offers its own options for social survival, including the promotion of new political leaders and the establishment of alternative formats of political activity (including armed struggle against the enemy). In other words, in the event of a critical and destructive armed attack by an enemy, the state may temporarily cease to exist. However, society remains. Even a fragmented society shows remarkable resilience and first focuses on improving its own well-being, then on restoring statehood. This proves that a mature civil society, with a deep understanding of national values and interests, is the main customer of the state-building project over time. There is a revival of the nation, including its implementation at a mature stage of development of the state-civil subproject of "national security."

However, it is impossible to predict in advance how civil influence will affect the state within the context of collectively defending society's security and defense features. Civil society's spontaneous and forceful actions on these issues cannot be anticipated or organized beforehand. This creates an additional form of social uncertainty regarding civil society's involvement in national security activities.

Uncertainty 6. The extent to which a sovereign state delegates security powers to international organizations with names that include the word "security." Russia's large-scale aggression against Ukraine has highlighted the striking weakness of most international security organizations, which proved unable to prevent the Russian invasion or lessen its effects. This includes the UN Security Council and the OSCE, whose international regulatory abilities remain outdated, stuck in the last century. When considering the aggressor, Russia faced a similar situation: during the war with Ukraine, the Collective Security Treaty Organization, established by Russia's own initiative in advance, offered little assistance. The only effective mechanism was NATO, which prevented the conflict from spreading to Alliance territory and facilitated the ninth enlargement through the accession of Finland and Sweden.

The recent history of Ukraine has added to the list of uncertainties about national security and defense the uncertainty of hybrid warfare, which, in its structure, function, resources, and other aspects, is a complex improvisation. The aim of hybrid warfare is no different from that of hot warfare: to weaken or destroy the enemy state. The essence of hybrid warfare lies in the deliberate development (hybridization, crossbreeding) of non-traditional strike methods — such as military, informational, diplomatic, economic, environmental, network, cybernetic, civil, partisan, and terrorist tactics — and their selective or widespread use. This results in a mix of conventional and unconventional combat operations, military, quasi-military, diplomatic, sanctions, financial, energy, trade, technological, cyber, and other forms of struggle; an expanding range of participants (military personnel, private armies, mercenaries, guerrillas, militias, terrorists, etc.); and a "blurring" of the start and end points of conflicts, often without official declarations of war or surrender. Notably, significant combat occurs in the information domain (information-psychological, propaganda), utilizing any and all available means to influence the minds of individuals and groups against whom this warfare is conducted.

It becomes clear that the number of uncertainties in the confusing format of hybrid warfare is excessive and cannot be addressed with linear analysis methods like "front – rear," "friend – foe," "non-interference – collaborationism," etc. There is an urgent need for a new security mindset based on processing vast amounts of information and extracting rational components capable of responding to current pressing issues of national security and armed conflict.

The combination of uncertainties and the threats they pose that humanity faced at the beginning of the 21st century is seen as unique, unprecedented, and especially dangerous. Modern science introduces new conceptual approaches to social relations under uncertainty, helping to understand social situations with ambiguous early signs or poor predictability, which can lead to particularly destructive consequences. One of them is the concept of a VUCA world, the acronym standing for Volatility, Uncertainty, Complexity, and Ambiguity [7]:

- Volatility – the situation changes quickly and chaotically; based on the available data, it is impossible to predict the next situation or plan further steps.
- Uncertainty – there is a lack of predictability, consistency, and understanding of the cause-and-effect relationships between causes, problems, and events that are formally separated in space and time; the future becomes unpredictable due to the inability or limitations of using past experience; the chance of disruptive changes in the social environment increases.
- Complexity – an avalanche-like accumulation of contradictory facts, assessments, and proposals; the consequences of mixing diverse intellectual constructs (positions, assessments, proposals) are chaos, confusion, and disorder in social relations, undermining orderly structures and greatly complicating management activities.
- Ambiguity – subjective interpretations of the situation and incorrect perceptions of the problem dominate, leading to a superficial attitude towards it; different authors arbitrarily mix verbal descriptions of the problem. As a result, the social evolution in space and time cannot be monitored linearly based on unambiguous judgments.

Despite the importance of each of these elements, uncertainty is considered the main component of a VUCA world. It is interpreted as vagueness, incompleteness, ambiguity, and unpredictability of a developing situation, which can only be partially or not at all controlled by the party concerned. As a component of most social systems and processes, uncertainty reflects the limited scope of conscious human participation in transpersonal processes and exists independently of the current understanding of their essence and consequences. At the same time, uncertainty should be distinguished from fallacy and indeterminacy. A striking example of fallacy-based policymaking is Russia's military campaign against Ukraine, which began in 2014 and was intended to be a short-term affair. The campaign was based on a series of assumptions that were ill-conceived and overly optimistic for the Russian leadership. Ignoring the possibility of such errors created uncertainty, which led to both Russian and Western

politicians and experts underestimating Ukraine's potential for resilience and resistance on the eve of the Russian invasion. Generally, uncertainty often arises from a lack of information needed for decision-making or from not trusting that information and its sources.

The strategies for responding to the challenges of a VUCA world, which enable the social management entity (the state) to navigate uncertainty and act effectively in unclear situations, are proposed elements of the reverse VUCA concept [8], where:

- Vision — a clear perception and understanding of the long-term direction that enables the organization to weather the "shake-up." Vision is a crucial step toward stabilizing the situation, capable of inspiring all stakeholders to transform. Derived from vision are the following options: clarity of the set goal; faith backed by facts and evidence; consistency and focus on finding interrelationships, trends, and patterns of influence of external factors.
- Understanding — ongoing monitoring of expectations by those under the influence; developing new ideas and applying them practically; ability to cooperate; responding well to constructive criticism; mastering new IT technologies; understanding human behavior in stressful and demanding situations; understanding the motives behind individual actions.
- Creativity/Clarity — ability to simplify; application of systematic thinking based on a global view of the outcome, understanding how system elements interact and depend on each other; use of intuition; application of interdisciplinary knowledge; critical perception of events; flexibility to make changes; focus on innovation in any field and willingness to adopt innovative approaches.
- Agility – speed and flexibility in executing processes, which contributes to improving the efficiency of the organization; confidence in the need for innovation, the search for new and original ways to solve all issues, and the improvement of processes; decisiveness in decision-making; innovative thinking, networking; continuous improvement.

In the case of all of the above, the VUCA acronym is equally applicable. Yet, here it offers solutions to the underlying challenges

dictated by uncertainty. The VUCA factor can and should be considered as a guiding element in building national security theory and practice. Its implementation should not be hindered by the "domain" limits, "threat passports," or other elements of the static perception of the national security environment.

There are currently three main ways to manage uncertainty:

- Quantitative analysis of a situation that contains an element of uncertainty; rational perception of the known, the understandable, the calculated, which limits the scope of objectifying of the unknown or uncertain. Ratio must prevail over irrationality, a prerequisite for making balanced political decisions.
- Locating boundaries of uncertainty. It's impossible to completely exclude it from the state management process. However, legal power centers are able to explain their actions in clear socio-political terms while safeguarding themselves against potential "black swans."
- Planning measures to reduce uncertainty. In particular, it is proposed to: control information in order to increase its reliability and prevent manipulation; clearly define problems, goals, and consequences before making a decision, during its implementation, and after its completion; form a broader and more active research community; involve additional (alternative) academic, academic-analytical, and media institutions in addressing security issues with elements of uncertainty.

Based on this, the following conclusions can be drawn regarding the advisability of making fundamental changes to the development and implementation of national security policy, taking into account the influence of uncertain factors [9]:

- Sudden and unpredictable changes in the security environment require greater flexibility in the development and implementation of public policy; stereotypical thinking based on past experience limits this flexibility.
- The need to respond to uncertainty requires clarifying the meaning of the nation as the object of protection, reviewing the hierarchy of national interests, and finding a new balance between national values and the needs of national security and stability.

- It is advisable to introduce more flexible but understandable approaches to determining the directions of national security, taking into account the peculiarities of risk transformation in modern conditions.
- The search continues for the optimal composition of the security and defense sector at the national level and ways to optimize state-civil society interaction in times of peace and war.
- There is a growing need to review the powers delegated by national governments to international security organizations and to search for effective crisis resolution mechanisms at the international level.
- The development and implementation of public policy should be based on adaptive management, which involves constant monitoring of the situation, identification of new trends, risks, and threats, and regular analysis of the compliance of public policy goals and objectives with changes in the security environment.
- Given the prevalence of nonlinear relationships in the system of social relations, conceptual approaches to assessing the effectiveness of state policy in the field of national security and developing tools for assessing its compliance with the principles of sustainability need to be updated.
- It is advisable to invest in the development of science. Security forecasting needs to become more sophisticated, primarily through the development of new methods (techniques) for forecasting changes in international relations and their impact on specific states in order to reduce the potential for uncertainty in their economic, political, environmental, spiritual, cultural, and other progress.

Regardless of the context in which we view the current chaos in international affairs, **it is important to realize that almost every state, even those that are mere observers, sees the situation in its own way.** It is telling that since the beginning of the 21st century, intelligence researchers, taking into account the "revolutionary changes" in the security environment, in the nature of threats and the nature of peace, as well as changes in the nature of warfare, emphasizing the changing nature of information, the speed of technological

change, and the variability of expectations not only of consumers of intelligence information but also of the general public, began to talk about the need for a "revolution in intelligence."

In July 2023, CIA Director William Burns gave a lecture at the Ditchley Foundation (UK), and in January 2024, in an article for Foreign Affairs, he outlined his strategic vision for the development of key trends in the modern world and in the field of intelligence [10, 11]. According to William Burns, the period of unquestionable US dominance is coming to an end, so Washington must rely on cooperation with partners and friendly alliances. In the intelligence field, the main partners of the United States are the United Kingdom and other members of the Five Eyes intelligence alliance (a strategic partnership between the United States, the United Kingdom, Australia, New Zealand, and Canada in the field of intelligence).

According to William Burns, there are three key trends in the modern world.

First, there is the challenge of strategic competition from a growing and ambitious China and from Russia, which constantly reminds us that a declining power can be at least as destructive as a rising one. According to William Burns, the main long-term threat to the US is China, the most serious adversary of the United States in the geopolitical and intelligence domains. Unlike Russia, China has the economic, diplomatic, military, and technological capabilities to reshape the world order. With this in mind, the CIA has established a China Mission Center, whose activities are focused exclusively on monitoring China and coordinating with all other US intelligence agencies on matters related to the PRC. Over the past two years, the CIA's spending on China has doubled. As noted by William Burns, US intelligence is, on the one hand, strengthening its capabilities to compete with China around the globe, and on the other hand, trying to maintain communication with China to avoid dangerous misunderstandings and accidental incidents.

Burns stressed that the problem is not China's rise as such, but the accompanying activities. President Xi is beginning his third term with more power than any Chinese leader since Mao. Rather than

using that power to strengthen, revitalize, and renew the international system that enabled China's transformation, he seeks to rewrite it.

He also stressed that the most immediate and acute geopolitical challenge to the international order today is Vladimir Putin's full-scale invasion of Ukraine. Although, as Mr. Burns noted, Russian aggression is a difficult test, the only country that intends to change the international order is China, and, moreover, has the economic, diplomatic, military, and technological power to do so.

Burns believes that Putin's war has been a strategic failure for Russia, as its military vulnerabilities have become apparent; its economy has been devastated; it faces a future as China's "junior partner" and "economic colony"; and its revanchist ambitions have been rebuffed by a North Atlantic alliance that has grown in size and strength.

Second, there are transnational problems such as the climate crisis and global pandemics, which are beyond the capacity of any single country to address and are becoming increasingly existential.

COVID has shown every government the danger of being dependent on a single country for vital medical supplies, just as Putin's aggression in Ukraine has clearly shown every government the risks of being dependent on a single country for energy supplies. In today's world, no country wants to be at the mercy of a cartel for an important mineral or technology, especially a country that has demonstrated the will and ability to deepen that dependence and weaponize it. The answer to this question is not to disconnect from an economy like China's, which would be foolish, but to wisely reduce risks and diversify by ensuring sustainable supply chains, protecting our technological advantage, and investing in industrial capacity.

And third, it is a technological revolution that is changing how we live, work, fight, and compete, with opportunities and risks that we cannot yet fully understand.

In this regard, Burns emphasizes that advances in computer-related technologies — from chips to quantum and AI — are leading to breakthroughs of extraordinary scale and scope. In just a few months

since the first public release of ChatGPT in November last year, we have seen newer models outperform humans on graduate school entrance exams and in evaluating doctor-patient interactions in medical training programs.

Leadership in technology and innovation has been the foundation of our economic prosperity and military strength. It has also been critical to establishing rules, norms, and standards that protect our interests and our values. Our Chinese rivals understand this as well as anyone else, and so it is not surprising that they are investing heavily in cutting-edge technologies as a central dimension of our strategic competition.

Illustratively, the U.S. Intelligence Community's annual report on global threats to national security (Annual Threat Assessment of the U.S. Intelligence Community. March 2025) states, "Russia, China, Iran and North Korea—individually and collectively—are challenging U.S. interests in the world by attacking or threatening others in their regions, with both asymmetric and conventional hard power tactics, and promoting alternative systems to compete with the United States, primarily in trade, finance, and security. They seek to challenge the United States and other countries through deliberate campaigns to gain an advantage, while also trying to avoid direct war. Growing cooperation between and among these adversaries is increasing their fortitude against the United States, the potential for hostilities with any one of them to draw in another, and pressure on other global actors to choose sides. [12].

In addition, the above-mentioned report emphasizes that the PRC is likely to continue to position itself as the country with the upper hand in a potential conflict with the United States. The PRC will continue to pressure Taiwan to reunify and will continue to conduct large-scale cyber operations against US targets for both espionage and strategic advantage. China will likely attempt to sufficiently restrict the activities of Chinese companies and criminal elements that supply and illegally traffic fentanyl precursors and synthetic opioids to the United States, unless more aggressive measures are taken by law enforcement agencies.

Beijing will continue to strengthen its conventional military capabilities and strategic forces, intensify competition in space, and maintain its industrial and technology-intensive economic strategy to compete with US economic power and global leadership.

China poses the most comprehensive and potent military threat to U.S. national security. The PLA is developing a unified force capable of full-spectrum warfare to counter U.S. intervention in regional conflicts, project power globally, and defend what Beijing considers its sovereign territory. A significant portion of China's military modernization efforts is focused on developing counterintervention capabilities tailored to all aspects of U.S. and allied military operations in the Pacific region. Beijing will focus on achieving key modernization milestones by 2027 and 2035, aimed at transforming the PLA into a world-class military by 2049.

Of particular note is that China is using an aggressive nationwide approach combined with state control of the private sector to become a global scientific and technological superpower, surpass the US, promote self-sufficiency, and achieve further economic, political, and military advantages. Beijing has prioritized technology sectors such as advanced energy, AI, biotechnology, quantum computing, and semiconductors, challenging US efforts to protect critical technologies by tailoring restrictions narrowly to address national security concerns. China is accelerating its scientific and technological progress through a range of legal and illegal means, including investment, acquisition, and theft of intellectual property, cyber operations, talent recruitment, international cooperation, and sanctions evasion.

In turn, on March 19, 2025, the European Commission presented the "White Paper for European Defence – Readiness 2030" [13].

The international order is changing. A new one will emerge as early as the second half of this decade. Europe must actively participate in these processes to avoid the danger of becoming a "passive recipient" of the consequences of the new order, including the prospect of full-scale war. The challenges to European security are strategic in nature and require a strategic response. The traditional spectrum of different types of security threats is rapidly expanding, and the

interconnections between them are intensifying, as evidenced by repeated cases of terrorism and violent extremism, hybrid attacks, and the actions of international organized crime groups and cybercriminal networks. There is evidence of links between criminal groups and hostile state actors, which easily cross borders thanks to new technologies. Due to their geographical proximity, European states are constantly confronted with migration caused by the effects of war and climate change in North Africa and the Middle East. The Arctic is becoming a new arena for geopolitical competition in the north of the continent.

Russia poses a serious strategic threat on the battlefield, forcing Europe and its partners to face the reality of intense, large-scale mechanized warfare on the European continent, which has not been seen for 80 years. Russia, which is the most heavily armed European state, is building a military economy focused on achieving its military goals through industrial mobilization and technological innovation. In addition, it is scaling up its military economy with the support of Belarus, North Korea, and Iran. The Russian Federation is making it clear that it remains at war with the West. And if it is allowed to achieve its goals in Ukraine, its territorial ambitions will extend beyond that country.

Hybrid threats are intensifying, such as cyberattacks, sabotage (particularly in the Baltic and Black Seas), electronic interference in global navigation and satellite systems, disinformation campaigns, political and industrial espionage, and the weaponization of migration. Geopolitical rivalry has not only led to a new phase in the arms race but has also triggered a global technology race. Technology will be a key feature of competition in the new geopolitical environment. A number of critical and enabling technologies (AI, biotechnology, quantum technology, robotics, hypersonic technology) are key components of both long-term economic growth and military superiority.

Given the fundamental changes in the strategic environment, Europe needs to build up sufficient deterrence capabilities to prevent potential aggression. The EU recognizes the responsibility of member states for their own armed forces: from doctrine development to

deployment characteristics and requirements. The EU has significant potential to support and coordinate efforts to strengthen the EU's defense industrial base and overall defense readiness through:

- Promoting closer cooperation and effective scaling of the European defense industry in the development, production, and promotion of weapon systems.
- Increasing the effectiveness, interchangeability, and interoperability of weapons, reducing costs by avoiding competitive procurement and improving the purchasing power of Member States, and ensuring stability and predictability through long-term industrial orders.
- Supporting dual-use infrastructure for mobility, space communications, navigation, and surveillance.
- Promoting various forms of partnership.

Thus, we can conclude that strategic competition, common transnational imperatives, and an unprecedented technological revolution in human history are creating an extremely complex international landscape. This undoubtedly draws attention to changing approaches to the role of intelligence in this transformed world.

4.2. The Concept of Intelligence Activities in Modern Conditions

The modern world is changing rapidly and irreversibly. Turbulence and tension in global politics and economics continue to grow. The familiar international order is becoming a thing of the past. The existing system of international relations and security, unable to withstand the hybrid challenges and threats of the 21st century, is currently undergoing fundamental transformations. This has further accelerated the emergence of a new global architecture of security and international relations.

In the context of contemporary global challenges and threats to international and national security, the international environment has undergone a transformation that has revealed a number of political, security, economic, and humanitarian problems that cannot be adequate-

ly assessed and overcome at the level of individual states alone. Their solution lies in the international political sphere and in the international security environment shaped by states that drive globalization.

The 21st century has seen the restoration of a great power, imperial type of geopolitical mentality, which, based on the experience of the historical past, offers the ideal of state development as the creation of "great empires" and mechanisms for their domination over "medium" and "small" states, as well as non-state political forces. This is particularly true of Russia and China, which in the 21st century are trying in various ways to implement the idea of a "great power renaissance." At the same time, it should be borne in mind that in postmodern conditions, great power geopolitical mentality has undergone changes: its orientation towards maximum possible territorial domination is concealed by information noise about the need to construct "great political spaces" capable of creating better conditions for meeting the socio-economic, political, cultural, and other needs of subjugated peoples and nations (the latter are not prohibited from having their own "decorative" statehood, the boundaries of which are to be regulated by the new metropolitan power).

Russia's unprovoked large-scale invasion of Ukraine has underscored that the era of inter-ethnic/inter-state competition and conflict is not a thing of the past, but has instead become a defining feature of the current era.

The strategic competition between the US and its allies, China, and Russia over what kind of world will emerge makes the next few years critically important, particularly in the context of Russia's actions in Ukraine, which threaten to escalate into a broader conflict between Russia and the West.

The "Ukrainian question" continues to dominate the assessment of the security environment, remaining high on the agenda and directly or indirectly affecting most areas and directions of international and regional security.

In this context, NATO's latest imperative – the imperative of cognitive superiority, which is intended to ensure the Alliance's strategic advantages – stands out. Cognitive superiority is one of the key

emphases that is present in one way or another in the Alliance's latest documents. In particular, a notable feature of The NATO Warfighting Capstone Concept (NWCC, 2021) [14] is that the "Concept..." refers to the future, up to 2040. Among other things, it notes a number of important points: the latest (and, accordingly, future) operational environment requires the Alliance to adopt a new way of thinking, organizing, and acting, and among its main tasks is to focus on military superiority and actively shape the "operational" environment, taking into account the specifics of its "constant expansion" and the activities of both traditional and non-traditional actors. Understanding the operational/security environment requires continuous scanning of the horizon — gathering information, studying the strategies of its participants, their approaches to warfare, assessing plans and intentions, strength and capability development for possible changes in the modes of action of all actors in the environment. Taking into account the basic premise of the NWCC, according to which the Alliance's future combat operations will be "multi-regional, multi-dimensional (physical, virtual, cognitive) and multi-domain operations" (i.e., on land, in the air, at sea, in cyberspace, and in space) in conditions where "border challenges" will only increase, when the boundaries between "domains" will effectively be erased, the idea of cognitive advantages takes on considerable importance.

The cognitive dimension of NATO's actions, as can be concluded from the NWCC, involves:

- Regarding the enemy, better knowledge and, consequently, understanding of the strategic environment, which will be "more demanding."
- Regarding NATO members – not only the Alliance's commitment to excellence and maneuverability (based on the uniqueness of NATO's military, ethos, culture, diversity, desire for initiative and victory in all circumstances over any adversary), but also, above all, possession of information and, accordingly, thinking that surpasses the adversary in speed (is "out of step") to recognize, take risks, make decisions, and act faster (than a potential adversary). The multifaceted cognitive dimension is the foundation for ensuring the abil-

ity of NATO members to "promote and utilize mutually supportive and familiar relationships and partnership opportunities"; the ability to think, plan, predict, and adapt for the sake of being able to "endure as long as necessary" in the course of strategic competition and in any conflict situation.

Cognitive superiority is declared a priority for the Alliance in the document and is interpreted as "understanding the operational environment and the capabilities of the adversary, the capabilities of the Alliance, and the objectives" as a "critical capability" aimed at "improving situational awareness and strategic forecasting" to "expand knowledge and understanding" in order to ultimately achieve objectives.

The imperative of cognitive superiority is not considered in isolation, but in context – in close connection with other imperatives of military operations, such as:

- Multilayered resilience, which involves the ability to absorb shocks and fight at all levels — military, civil-military, and military-civilian.
- Projection of influence and power, the essence of which is to create a positive environment that takes into account the strengths of the Alliance, including creating options and imposing dilemmas on the adversary.
- Integrated multi-domain defense, which is the understanding by commanders of the multi-domain operational environment for the sake of rapid and effective action.
- Inter-domain team, which is to ensure the unity of the Alliance in decision-making and countering threats "in any domain, regardless of their origin or nature" and which will possess flexible and asymmetric thinking in commanding missions in 2040, continuously reinforced by reliable and constantly updated communication and information systems.

In characterizing "leaders and headquarters," the NWCC emphasizes the need for such individuals (one might say superhumans) who are "able to cope with the speed, complexity, and be data- and technology-oriented" of the security environment of the future. In

addition, there is an interesting emphasis on gender and generations: NATO and its allies must use "gender and diversity as force multipliers" and avoid the risks associated with the generation gap. Thus, achieving cognitive advantages for NATO and its allies effectively precludes discrimination based on gender or age. However, in each case, the intellectual or cognitive abilities/aptitudes of the individual (along with their values or cultural priorities) are taken into account, rather than, for example, their gender specificity (i.e., whether the individual is transgender, lesbian, gay, non-binary, cross-dresser, etc.), or their previous experience, which in the 21st century, with the emergence and development of new technologies used/to be used on "day zero," is rapidly losing its relevance. Therefore, the "breadth of diversity" (in the language of the Concept) is important, but, as can be assumed, with significant reservations.

As stated in the NWCC, a special role is assigned to the training of individuals needed to perform tasks relevant to NATO (including in the cognitive domain), in particular during their studies at the NATO Defense College (NDC) in Rome and the NATO School in Oberammergau, Germany, which are clearly are considered a reliable foundation for moulding (shaping and developing) the minds of those who already provide and will continue to provide (after 2040) cognitive advantages to NATO and its allies, guided by the principle of the NDC's founder, General Dwight D. Eisenhower: "Develop individuals, both military and civilian, so that they have a complete understanding of the many complex factors involved in creating an adequate defense posture for the North Atlantic Treaty area." The success of future military operations, as envisaged in the document, will be "entirely data-driven." Therefore, according to the strategists' plan, there should be a broad exchange of high-quality data within the Alliance, the processing of which should be continuously improved. It is envisaged to combine "all sources of information and intelligence," expand analytics within the framework of military-strategic decision-making processes, and achieve "integrity and consistency of information flows." In addition, the NWCC encourages Alliance members to share technological intelligence data and scan the hori-

zons of new scientific and industrial developments both within and outside NATO in order to "identify areas of potential advantage" (particularly technological).

Another important aspect of the NWCC is its emphasis on a unique learning mechanism (to achieve cognitive advantages), which involves "continuous training" based on a "culture rooted in the Alliance's armed forces." It is precisely this continuous training of personnel based on the established culture that, according to Alliance strategists, is the asset that will allow them to surpass others. It has two important components: the first is the ability to develop complex scenarios, and the second is to practice developing a range of options for such scenarios and, accordingly, a range of decision-making options. The requirement for the training process is very specific: training exercises must use "live and advanced models and simulation constructs," which will subsequently ensure "the identification of areas for improvement, strengthen confidence in new opportunities and plans," support the development of work gaming, experimentation, as well as exclusive – realistic (!) in nature – training that takes into account the "day zero" factor that may occur (before or after 2040).

Regardless of the context in which we view the current chaos in international affairs, **it is important to realize that almost every state, even those that are mere observers, sees the situation from its own perspective.** Notably, since the beginning of the 21st century, intelligence researchers, taking into account the "revolutionary changes" in the security environment, in the nature of threats and the nature of peace, as well as changes in the nature of warfare, noting the volatility of information, the speed of technological change, and the variability of expectations not only of consumers of intelligence information but also of the general public, began to talk about the need for a "revolution in intelligence."

Indeed, Anthony Vinci, former Chief Technical Officer and Deputy Director of the U.S. National Geospatial-Intelligence Agency, noted in his article "The Coming Revolution in Intelligence Affairs: How Artificial Intelligence and Autonomous Systems Will Transform

Espionage" (2020): "For all of human history, people have spied on one another. To find out what others are doing or planning to do, people have surveilled, monitored, and eavesdropped — using tools that constantly improved but never displaced their human masters. Artificial intelligence (AI) and autonomous systems are changing all of that. In the future, machines will spy on other machines in order to know what other machines are doing or are planning to do. Intelligence work will still consist of stealing and protecting secrets, but how those secrets are collected, analyzed, and disseminated will be fundamentally different." [15]

In addition, the work "Intelligence Analysis in the Digital Age" (2021) [16], within the concept of the "digital era," notes an increase in changes and complications (in terms of "challenges-threats-risks") that affect the speed of information dissemination: new technologies have reduced the time it takes to disseminate information to virtually zero. This state of affairs leads to decisions being made in increasingly unfavorable conditions, when the demand for timely, relevant, and reliable intelligence is steadily growing, and the time for making adequate decisions is minimized. Accordingly, the development of timely policies in an extremely volatile world also becomes a challenge for leaders, states, and communities.

Another challenge of our time for intelligence and information work is related to the problem of "big data" collected in today's diffuse, multipolar environment. In the 2024 book by Miah Hammond-Errey, "Big Data, Emerging Technologies and Intelligence: National Security Disrupted," [17] argues that big data is transforming intelligence knowledge production, as well as the relationship between the intelligence community and the public, and calls into question the separateness (isolation) of internal and external intelligence gathering. This, of course, requires constant reconfiguration of the intelligence community of a state or states.

"Big data" is the result of integrating intelligence data from multiple sources. Back in 2015, American analysts, reproducing the diversity of data used in the analysis, pointed to the use of information from numerous data generators: in particular, MQ1 Predator "combat

air patrols," hyperspectral sensors with intensive data volumes, light detection or range sensors, which, in turn, was supplemented by signal intelligence (SIGINT) sensors, information from moving target indicator sensors, infrared sensors, and unconventional measurement and signature sensors (Measurement and Signature Intelligence, MASINT). The "big data" puzzle is based not only on a multitude of sources, but also on a whole range of disciplines that integrate both the aforementioned SIGINT and MASINT, as well as human (or agent) intelligence (Human Intelligence, HUMINT) and geospatial intelligence (Geospatial Intelligence, GEOINT), and, of course, open source intelligence (OSINT).

Thus, even today, the challenge in collecting, integrating, and analyzing information may be the inability to move away from traditional linear approaches to data collection and processing (whose weakness is the unintentional devaluation of information and, as a result, the emergence of "strategic surprises"), as well as to further assessment and forecasting, which can lead to a kind of "intelligence failure."

Thus, the following features of intelligence activities in modern conditions can be identified:

1. Introduction and use of new technologies and innovations. The digital technology revolution has had a greater impact than the industrial revolution or the advent of atomic energy in their time. With this in mind, the CIA has established a Special Technology Center, which actively cooperates with the private IT sector, and has introduced a new position of Chief Technology Officer of the CIA for the first time in history.

One of the most revolutionary technologies for gathering military intelligence today is the integration of drones and satellites. The use of these innovative technologies has not only given the armed forces a number of significant strategic and tactical advantages but has also transformed the landscape of military intelligence. The introduction of modern algorithms has made it possible to analyze collected data in real time, and thus to identify threats on the battlefield more quickly and effectively.

Satellite technology has been an important component of intelligence for several decades. Satellites orbiting high above the Earth provide extensive coverage, data collection, and communication capabilities, making them indispensable in modern warfare. The synergy expressed in the integration of drones and satellites for intelligence gathering has marked a new era in the development of intelligence activities.

The introduction of AI-based technologies plays a significant role in the transformation of its systems, enabling the analysis of large amounts of data and generating important information for management decision-making. Using AI technologies for intelligence analysis, it is possible to identify potential threats, map enemy activities, assess the geopolitical situation, and make quick and informed decisions.

The main advantages of AI-based data analysis in intelligence are in-depth situational awareness, improved forecasting capabilities, and accurate threat assessment.

Defense intelligence systems can use cognitive AI to support military leadership decision-making, assisting in complex strategic planning and risk assessment. Cognitive computing can be applied in military intelligence in the following areas:

- Natural Language Processing (NLP) – NLP algorithms can process text data, enabling defense intelligence systems to extract information from large volumes of unstructured documents.
- AI – AI-based virtual assistants help military leaders organize information, make inquiries, and make decisions in real time, saving valuable time in critical situations.
- Scenario modeling – AI cognitive systems analyze various parameters and simulate the implementation of different scenarios, helping the armed forces predict outcomes and develop effective strategies.

The integration of AI with autonomous systems and robotics is leading to significant changes in intelligence activities. Among the most significant advantages of introducing AI into autonomous systems are the following:

- They perform visual surveillance, collect and analyze data much more efficiently, minimizing the risk to personnel.
- These systems can detect, track, and identify potential targets with greater accuracy, minimizing the possibility of unnecessary damage to civilian infrastructure.
- Autonomous systems equipped with AI optimize logistics and supply chains, ensuring the timely delivery of resources to the front lines.

2. Cooperation with the private sector and use of social networks.

Today, new technologies allow non-governmental entities and individuals to collect and analyze intelligence data sometimes better and faster than government agencies. Commercial entities launch hundreds of satellites every year. More than half of the world is online, producing and receiving open-source intelligence, even if they are unaware of it. According to a 2019 World Economic Forum report, Internet users post about 500 million tweets on Twitter and 350 million photos on Facebook every day [18, 19].

In particular, the CIA has created a unit focused on building partnerships with the private (non-governmental) sector in order to obtain innovations that provide a competitive advantage.

In addition, social networks are actively used. Thus, as part of countering Russia, US intelligence agencies have intensified their recruitment efforts (in particular, using Telegram) among Russian citizens dissatisfied with the Kremlin's policies.

3. Controlled disclosure of sensitive information.

"Strategic disclosure," the deliberate public disclosure of certain secrets in order to undermine competitors and rally allies, has become a powerful political tool. Using it does not mean recklessly jeopardizing sources or methods of obtaining intelligence, but rather means sensibly resisting the reflexive desire to keep everything secret.

4. Partnerships and personal contacts with representatives of special services of other countries.

Personal contacts and partnerships are a kind of exploratory diplomacy that helps to align interests and support the efforts of politicians and diplomats to achieve the necessary results.

These meetings are an important means of protecting against unnecessary misunderstandings and unintended clashes, and they complement and support policy-making channels such as contacts between heads of state.

5. Investment in people (IA personnel).

Professional training of personnel is becoming increasingly important in today's environment and is a key factor in strengthening intelligence agencies (services).

It is necessary to attract and retain technological talent, improve compensation packages, and encourage more flexible career models so that officers can move to the private sector and then return.

It is telling that, according to the website of the Office of the Director of National Intelligence, of the more than 165 vacancies (in the fall of 2024), a huge number (apart from doctors, lawyers, and translators) were for specialists capable of working directly in the field of intelligence. An analysis of the positions and, accordingly, the areas of work identified by the CIA (in one position or another) allows us to highlight certain specifics of the CIA's "desires" in the current environment. Thus, the CIA's focus in terms of the knowledge, skills, and abilities of specialist candidates was on:

- Knowledge, abilities, and skills in various fields (for example, a lawyer position requires working "at the intersection of law and advanced technologies," while a methodologist-analyst must be able to "develop methods to improve the accuracy of analysis and intelligence gathering using statistical, econometric, and mathematical estimates," perform geospatial modeling, etc.);
- A bachelor's degree is required (in particular, for accountants, cartographers, polygraph examiners, or case officers who "covertly identify, evaluate, develop, recruit, and service non-US citizens who have access to foreign intelligence data vital to US foreign policy and national security");
- A mandatory master's or higher degree (for "methodologist-analysts," "life scientists and biotechnology experts," and lawyers with a "Doctor of Jurisprudence" degree exclusively from law schools accredited by the American Bar Association) for psycholo-

gists – a bachelor's or master's degree for "protective agents" who "are part of a team that provides armed protection for RS leaders around the world 24/7/365";

- An associate professor degree (for corporate IT specialists who "provide the agency's mission partners with advice, analysis, and solutions regarding technology products, programs, data and system access, and software issues"; for "physical and technical security" officers).
- Multidisciplinary expertise (i.e., not only the position of "intelligence officer," but also "multidisciplinary intelligence officer" or "DST Data Scientists" in the field of data collection and use, who are able to collect data "from many systems and data types" in order to obtain "key mission information"); or "DDI Data Scientists" who "solve critical data problems by creating optimal data pipelines, analyzing and transforming data, and delivering data to systems to advance the CIA's intelligence mission");
- Analytical skills (military and civilian positions: personnel analyst; human resources analyst; intelligence analyst; military analyst; political analyst; lead analyst; data collection analyst; data analyst; human resources analyst; targeting analyst; technical targeting analyst; business analytics officer; economic analyst; cyber threat analyst; software analyst; IG auditor/software analyst; IG-IT auditor/software analyst; supervisory IT auditor/IG software analyst, etc.);
- Strong research skills (research component in the skills/abilities of specialists for positions: science, technology, and weapons analyst; materials research scientist; "power supply engineers and scientists"; "microelectronics research scientist"; intelligence scientists who "research, write, and teach all aspects of CIA history... have access to source material. Their works include short essays or book-length histories," etc.);
- Proficiency in cutting-edge technologies ("artificial intelligence specialist"; "augmented reality specialist" who uses "their expertise to develop opportunities for virtual, augmented, and sensor-enhanced environments using game mechanics, haptic devices, and/or immersive glasses").

6. Budget.

Priorities are not meaningful unless they are backed by a budget.

Despite the revolution in digital technology and the rapid development of technical intelligence, human intelligence remains a priority for any intelligence service. This is because there will always be secrets that we can only learn about through human sources, and covert operations that only humans can carry out. This requires human intelligence officers to undergo intensive training, work as a team, and possess impressive creativity and a thirst for risk.

The above points are closely intertwined with the provisions of the US National Intelligence Strategy, published in August 2023 [20]. The document identifies six main areas of development for US intelligence, namely:

- Strengthening the role of intelligence in connection with the intensification of strategic competition between the US, China, and Russia. It is stated that only China has both the intentions and capabilities to compete with the US, while Russia is a source of constant threat to regional security in Eurasia, as well as a destabilizing factor at the global level. In the context of strategic competition, the main task of US intelligence is to ensure US leadership in technology and innovation, primarily through open source intelligence, big data, AI, and advanced analytics. To this end, the U.S. intelligence community (IC) must intensify cooperation with allied and partner intelligence services, as well as with the non-governmental and private sectors.
- recruitment, professional development, and retention of talented US IC personnel. The most valuable personnel are those who are technically trained and talented but, due to organizational, bureaucratic, and other constraints, are either unable to find employment in intelligence or resign after a short period of service. To speed up recruitment, it is planned to modernize the US intelligence community's employee selection and recruitment system, and to enhance professional development, it is considered appropriate to continue practicing joint missions for representatives of various intelligence agencies, who will participate in them on a rotational basis.

- Developing interoperable and innovative solutions to build new capabilities for the US IC. The result of implementing these solutions should be the creation of unified units responsible for purchasing the necessary property and equipment; the introduction of a centralized automated system for submitting purchase requests and a unified system for concluding contracts for the performance of work. The key to success is considered to be the formation of a corporate culture within the US IC that will be focused on finding new tools, processes, and standards that will help perform labor-intensive tasks through productive human-machine (AI) interaction. The fundamental principle is data-centricity, which involves a significant increase in the availability and standardization of intelligence information, as well as the ability to search for and extract specific data from existing information volumes. This requires deeper integration of the US IC's research, technical, analytical, and collection units.
- Expansion, diversification, and strengthening of partnerships in the field of intelligence. The creation of a network of allies and partners significantly enhances the operational and analytical capabilities of the US intelligence community. An important condition is the intensification of intelligence sharing at the regional and local levels. At the same time, the US IC must rethink and improve procedures for sharing information with non-governmental and sub-national institutions, as their role has grown significantly, especially in the area of protecting critical infrastructure from cyber threats.
- Increasing the level of expertise on transnational challenges such as climate change, drug trafficking, financial crisis, supply chain disruptions, corruption, unknown diseases, and disruptive technologies. In this context, the US IC plans to engage the best experts who have a high level of knowledge in their fields and are capable of formulating proposals for the state leadership to make appropriate strategic decisions.
- Ensuring the sustainability of the US IC. To this end, it plans to modernize and expand its intelligence infrastructure to improve its ability to detect and warn of the most dangerous threats, such as pandemics, massive cyberattacks, climate change, and terrorist acts. At

the same time, the intelligence infrastructure must ensure not only the stable functioning of intelligence, but also the ability to strike back and quickly recover in the event of an attack.

In the context of the digitization of intelligence activities, the US IC Data Strategy for 2023–2025, adopted in July 2023, which outlines the main directions of the US Intelligence Community's digitization policy, is also noteworthy [21]. According to the document, the new era is characterized by the data-centricity of the world. In this regard, US intelligence must implement the experience of leading commercial companies that organize their work according to the principles of agile2 and continuous learning. Against this backdrop, the importance of in-depth data analysis is growing in the interests of the fastest possible decision-making by state leadership. One of the most important tasks is to improve the format of intelligence information so that data can be perceived equally effectively by both humans (information consumers) and machines.

Until now, data itself has not been considered a key tool for intelligence activities at either the strategic or operational levels. The main problem is that US intelligence agencies are too slow to develop data capabilities such as comprehensive data collection and analytics, primarily using AI. To improve the situation, the US IC considers it appropriate to implement a data-centric approach, which will make it possible to improve the processes of integration, transportation, distribution, use, and maintenance of intelligence data.

The main directions for implementing the US IC's Data Strategy are as follows:

- The application of the E2E (end-to-end) principle in data management involves detailed planning, development, and implementation of uniform procedures for collecting, processing, distributing, and using information. To this end, a unified format for intelligence data (tags or labels) will be introduced in the US IC for further processing using AI, as well as standards for the generation, exchange, distribution, delivery, and protection of information.
- Ensuring the interoperability of data for timely delivery to the right consumer requires a paradigm shift in intelligence man-

agement from system-centric to data-centric. Whereas previously the main goal of intelligence management was to create an information architecture (computers, servers, networks, etc.), the focus of management is now on procedures for collecting, analyzing, and distributing information using AI. The data-centric approach should improve the quality of intelligence information, deepen its integration, and increase the accuracy of interpretation and interoperability. The use of AI should reduce the time required to collect and process the necessary information from weeks/days to hours/minutes.

- The development of partnerships in the field of digital innovation involves active cooperation between the US IC and foreign intelligence services, civil institutions, and academic circles to better understand information technologies and respond to changes in their development. It should be emphasized that until now, the cooperation of the US IC with the private sector and scholars has not been so important, given the rapid pace of the digital revolution, especially in the field of AI.
- Improving the data literacy of intelligence personnel. The transition to a data-centric model of the US IC's development is impossible without changing the education system and the training and professional development of intelligence personnel in the context of their understanding that working with data is the basis for the successful completion of any mission (task). Data literacy is recognized as one of the key professional competencies of both ordinary employees and senior intelligence managers.

4.3. The Place and Role of Non-State Actors in Intelligence Activities in the Context of Safeguarding National Interests

Currently, the foreign policy of any state is based on the information it has about socio-political issues, research into key problems in the political and social domains, analysis of strategies and tactics, and the implementation of political and socio-economic reforms. One of the main sources and processors of this information are intelligence

agencies, which help the state learn about its external environment and understand its own tasks in this area. Accordingly, civilian and military intelligence agencies focus on searching for, analyzing, and using information, both classified and obtained from open sources (OSINT). For a long time, states sought to retain a monopoly on intelligence activities. However, the first half of the 1990s saw the emergence of private entities that provided information and analytical services beyond business intelligence, not only to large corporations and individuals, but also to government agencies. Such organizations were called "private intelligence companies" (PICs), and public-private partnerships began to develop in this specific area of activity. According to rough estimates, there are several hundred PICs operating in more than 50 countries around the world [22].

A significant reason for involving PICs in ensuring the external component of national security was that private structures are generally more flexible and effective than state ones, particularly in economic relations. In addition, such a PIC contractor made it possible to reduce government spending on the maintenance of special services, as well as to resolve some sensitive issues while concealing the direct involvement of the state in them. PICs offer their services not only to government agencies, but also to large corporations and individual consumers [23].

The United States is considered the originator of the public-private partnership system in the field of national security, and the first PIC was the American global policy research center, RAND Corporation (Research and Development) [24]. It was founded on May 14, 1948, in Santa Monica, California, by Henry Harley Arnold, Donald Wills Douglas Sr., and Curtis LeMay as a partnership between the U.S. Air Force and Douglas Aircraft Company for the design of aircraft, rocket technology, and satellites. The RAND Corporation is considered one of the world's first think tanks or policy institutes, providing military advice to state leaders and the Department of Defense.

The history of the RAND Corporation dates back to World War II, when a large group of mainly scientists and engineers was formed

in the United States to wage war on the "technological front." In a relatively short period of time, this group created such innovations as the atomic bomb, radar, proximity fuses, and more. An analytical method of operations research was also developed and successfully applied, which made it possible to increase the effectiveness of air defense, bombing, and naval operations.

At the end of the war, when this team began to disband, the military decided to retain some of the most talented employees to continue developing military technology. General Henry H. Arnold, commander of the US Army Air Forces, created the RAND project with $10 million in funding for long-term planning of future weapons. In March 1946, Douglas Aircraft was awarded a contract to study intercontinental warfare using operations research. In May 1946, a preliminary design for an experimental space plane capable of circumnavigating the globe was released. On May 14, 1948, RAND was registered as a non-profit corporation under California law, and on November 1, 1948, Project RAND was officially transferred from Douglas Aircraft Company to RAND Corporation. Thus, Project RAND became the independent non-profit organization RAND Corporation, with initial capital provided by the Ford Foundation.

RAND's first major work was a study published under the title Preliminary Design of an Experimental World-Circling Spaceship. Although artificial Earth satellites were considered science fiction at the time, this 1946 document stated: "A satellite vehicle with appropriate instrumentation can be expected to be one of the most potent scientific tools of the Twentieth Century. The achievement of a satellite craft by the United States would inflame the imagination of mankind, and would probably produce repercussions in the world comparable to the explosion of the atomic bomb..." This successful prediction strengthened the prestige of the RAND Corporation. In mid-1957, the launch date of the first artificial Earth satellite was predicted with an error of only two weeks.

By the end of the 1950s, academic literature defined the differences between systems analysis and operations research, systems analysis and systems engineering, decision theory and operations

research, etc. The problems of applying scientific methodology to such "imprecise" areas as management, human decision-making, and organization were widely discussed. An example of an important achievement by the RAND Corporation in solving these scientific and applied problems is the development and widespread application of systems analysis. RAND Corporation experts conducted a series of fundamental research and development projects on systems analysis, focused on solving the loosely structured problems of the US Department of Defense. The creation of the B-58 supersonic bomber in 1952 was the first development delivered as a system. All this required the publication of scientific and educational literature.

The first book on systems analysis was published in 1956. It was published by RAND (authors H. Kahn and I. Mann). The methodology of systems analysis was developed in detail and presented in 1960 in the book by C. Hitch and R. McKean, The Economics of Defense in the Nuclear Age. It also includes an appendix on methods for quantitative comparison of alternatives for solving armament problems. Later, Charles J. Hitch (Assistant Secretary of Defense, President of the University of California) described the systematic approach to weapons selection in the United States.

In 1965, E. Quade's very thorough book "Analysis for Military Decisions" was published. It presents the foundations of a new scientific discipline — systems analysis. The book aims to justify methods for optimal selection when solving complex problems in conditions of high uncertainty. This book is a revised version of a course of lectures on systems analysis given by RAND Corporation employees to senior specialists of the US Department of Defense and Industry.

The same year saw the publication of S. Optner's book "Systems Analysis for Business and Industrial Problem Solving", which is full of new ideas and provides a complete and clear picture of system analysis with a description of the problems of the business world, the essence of systems, and the methodology for solving problems. The book was one of the first works published in our country that shed light on the state of this field in the United States. Academic disciplines in systems theory and systems analysis are normative and im-

portant elements of the education system in many higher education institutions around the world and in Ukraine.

As can be seen from the titles of the books, during the development of methods of systems analysis for the military sphere, it became clear that civilian problems — problems of firms, marketing, auditing, and others — also require the mandatory application of systems analysis methodology and a systems approach. The systems approach has become an important method of cognition, unlike the special techniques characteristic of the development of technology in the 16th-19th centuries. This was the second stage in the historical development of the systems approach in technology. A whole range of highly complex and sophisticated mathematical methods were developed, including linear programming, dynamic programming, problem prioritization, nonlinear programming, the Monte Carlo method, game theory, and others. In 1957, the book "System Engineering: An Introduction to the Design of Large-Scale Systems" by H. Good and R. Machol was published in the United States.

The RAND Corporation has done significant work on studying the problems of nuclear weapons proliferation, analyzing the economic, political, and technical aspects of building nuclear capabilities in various countries. The RAND Corporation was the first American institution to begin developing Cold War science using methods that involved intensive study of potential adversaries "from a certain distance." The RAND Corporation is also the developer of the concepts of "flexible response," "counterforce," and others. Its most notable contribution is the Mutually Assured Destruction (MAD) doctrine, developed under the leadership of then-Defense Secretary Robert McNamara, based on game theory.

MAD is a military doctrine according to which the use of weapons of mass destruction by two opposing sides will lead to the complete destruction of both sides, rendering any attempts to use the first strike doctrine meaningless. The word "mad" also means 'crazy' or "insane," and the term MAD was introduced by John von Neumann, a brilliant mathematician and consultant to the RAND Corporation. The doctrine of mutually assured destruction is a clear example of

Nash equilibrium, in which no armed party can either start a conflict with impunity or disarm voluntarily.

In 1971, a group of mathematicians from the RAND Corporation, led by Andrew Marshall, developed the first mathematically based National Intelligence Estimates (NIE), which contained the systematized results of processing intelligence and public data obtained from various sources. Now, the NIE is developed by the National Intelligence Council for the federal government. It is the consensus of all 18 components of the US intelligence community. Andrew Marshall, a prominent analyst at the US Department of Defense who predicted a number of important changes in the world, including the collapse of the USSR, the rise of China's geopolitical role, and the widespread use of robotics in military operations, was appointed head of the Pentagon's Office of Net Assessment in 1973. In this position, he lived through the Cold War, countless military conflicts, and 10 presidential elections.

The RAND Corporation has also made a significant contribution to the field of Artificial Intelligence (AI). RAND researchers developed many of the principles that were used to create the Internet. The RAND Corporation's experience in the military sphere led to the creation of the world-renowned Defense Advanced Research Projects Agency (DARPA) in the United States. In turn, DARPA's successful experience made it possible to create a similar structure for the U.S. National Intelligence (Intelligence Advanced Research Projects Activity, IARPA), as well as similar bodies in civilian ministries (government agencies), such as the US Advanced Research Project Agency for Education (ARPA-Ed). This systematic approach led to the opening of the Government Advanced Research Development Agency (GARDA) in 2018.

Today, the RAND Corporation is one of the world's most respected think tanks in all areas of public policy and management, national security and intelligence, from defense and international relations to education, health care, urban planning and infrastructure, transportation, energy, environmental protection, law, demographics, employment, and more. At the same time, RAND maintains close,

unofficial ties with its main client, the CIA. The corporation has about 1,700 employees from 50 countries who are experts in a wide variety of fields (economics, psychology, medicine, education, engineering, mathematics, computer technology, international relations, etc.). Among the corporation's employees were such well-known figures as Professor Francis Fukuyama, US Secretary of State Henry Kissinger, Secretary of Defense and CIA Director James Schlesinger, Deputy National Security Advisor to the US President James Steinberg, and the RAND Board of Directors included former U.S. Secretary of State Condoleezza Rice and U.S. Secretary of Defense Donald Rumsfeld. Thirty Nobel Prize winners have been involved in various projects of the corporation.

The RAND Corporation has offices in the United States: Santa Monica, California, where its headquarters and Frederick S. Pardee Graduate School are located; Arlington, Virginia; Pittsburgh, Pennsylvania; Boston, Massachusetts; and Washington, D.C. RAND also has American researchers living and working in more than 35 other states and the District of Columbia. In addition, it has offices in Cambridge (UK), Brussels (Belgium), Rotterdam (Netherlands), and Canberra (Australia). RAND's research clients include governments and government agencies in various countries, non-governmental organizations, and private companies.

The Rand Corporation is aptly portrayed in a book published in 2008 entitled "Soldiers of Reason: The RAND Corporation and the Rise of the American Empire." The corporation aims to solve problems in an interdisciplinary and quantitative way by translating theoretical concepts from formal economics and physical sciences into new applications in other fields, using and developing applied scientific research. A significant part of RAND's research involves national security issues. Many of the events in which RAND plays a role are based on assumptions that are difficult to verify due to the lack of details about RAND's work for defense and intelligence agencies.

After the collapse of the USSR, already in the new geopolitical conditions, in 1992, former CIA employees established the CTC International Group in Florida. Presumably, the group's personnel

composition led to limited public information about this PIC. A brief advertisement on the website states that the company works in the field of security and investigations and provides practical information to educate clients and help them make informed decisions [25]. Led by former CIA officers, CTC uses the intelligence cycle to provide private clients with high-quality intelligence that the US government uses to make decisions. Targeted research combined with professional analysis provides intelligence, not just "information," which separates the "nice to know" from the "need to know." CTC provides intelligence to CEOs, lawyers, and other decision-makers who need accurate, actionable, and effective intelligence. After all, knowledge truly is power.

CTC International Group specializes in business analytics, competitive intelligence, independent company verification, background checks, strategic intelligence, and support for complex litigation. The company has between 50 and 100 employees.

One of the most well-known and reputable PICs is Strategic Forecasting, Inc. (Stratfor), founded in 1996 by political scientist George Friedman [25]. In the early 1980s, he began conducting research on Soviet-American relations. In 1994, he founded the Center for Geopolitical Studies at Louisiana State University, which specialized in strategic forecasting. From 1996 to 2015, he headed Stratfor.

Stratfor's materials are referenced by influential media outlets, including CNN, Bloomberg, Associated Press, Reuters, The New York Times, Time, and the BBC. In 2001, Barron's magazine called Stratfor the "shadow CIA." Gradually, this PIC surpassed RAND in terms of its influence among corporations and government organizations and its popularity among journalists. The fundamental difference between Stratfor and RAND is that Stratfor was the first to create a global intelligence network focused primarily on corporations and a corporate approach.

Stratfor employees collect and analyze information about world events, focusing on security issues and geopolitical risks. They obtain information not only from the media and other open sources, but also from their own sources. In fact, this is human intelligence

(HUMINT). Based on the information collected, Stratfor analysts make economic and geopolitical forecasts. The company has about 100 employees.

In addition to researchers from various scientific fields, Stratfor involves experts with relevant practical experience in its work. For example, from 2004 to 2020, the company's vice president for counterterrorism and corporate security was Fred Burton, a former US Secret Service employee and later deputy chief of the Counterterrorism Division of the US State Department's Diplomatic Security Service. From 2013 to 2018, the vice president for customs intelligence was Bret Boyd, a former officer of the US Special Operations Command.

In 2012, Stratfor found itself at the center of a scandal sparked by the international organization WikiLeaks, founded by Australian journalist Julian Assange. He published more than 5 million of the company's emails and accused it of tracking the activities of international activist organizations on behalf of PIC clients, including The Dow Chemical Company and The Coca Cola Company, as well as US intelligence agencies. The materials stolen by hackers also mentioned Stratfor's contacts with the Israeli national intelligence service Mossad. After the controversial data leak, the company was forced to assure its clients that it would strengthen security measures and also offered a two-week free subscription to new mailings. Given the semi-public nature of the company's agent network, its partial disclosure did not lead to significant losses for the network or damage to PIC's reputation.

In 2015, Friedman became the founder and head of a new PIC, Geopolitical Futures (GPF). An analysis of the company's public publications and statements by this leading expert indicates certain changes in his political sympathies, which may have prompted J. Friedman to leave Stratfor, as well as inconsistencies in his strategic forecasts [26].

In May 2000, The Arkin Group LLC (TAG) was established [27]. The founders of this PIC are the former head of global operations at the CIA and renowned New York lawyer Stanley Arkin. TAG specializes in international crisis management, strategic intelligence,

investigative research, and business problem solving, using strategic information, predictive analysis, and data (HUMINT).

Jack Devine, founding partner and president of TAG, is a 32-year veteran of the CIA. He served as acting director and deputy director of CIA operations outside the United States from 1993 to 1995, where he oversaw thousands of CIA employees involved in covert missions around the world. In addition, from 1992 to 1993, Devine served as Chief of the Latin American Division and was the senior manager of CIA covert projects in Latin America. From 1990 to 1992, Devine headed the CIA's Counternarcotics Center, which was responsible for coordinating and building close cooperation between all major law enforcement agencies in the US and other countries in tracking global drug traffickers and criminal organizations. From 1985 to 1987, he headed the CIA's Afghanistan Task Force, which successfully countered Soviet aggression in the region. In 1987, he was awarded the CIA's Distinguished Officer Award for this achievement.

Devine's international experience in the US government included assignments in Latin America and Europe. During his more than 30 years with the CIA, he participated in the organization, planning, and execution of numerous covert projects in virtually all areas of intelligence, including analysis, operations, technology, and management. Devine has been awarded the Agency's Distinguished Intelligence Medal and several honorary awards. He is a recognized expert on intelligence and has written opinion pieces for The Washington Post, The Wall Street Journal, The Financial Times, Foreign Affairs Magazine, The World Policy Journal, Politico, and The Atlantic Monthly. He has also appeared as a guest on the National Press Club, CNN, CBS, NBC, MSNBC, Fox News, CSPAN, Bloomberg News, as well as the History and Discovery channels, PBS, NPR, and ABC Radio.

In the private sector, Devine has previously served on Kohl's Cyber Security Advisory Group, SAP National Security Services (NS2) Advisory Board, CyberCore Advisory Board, and Secretary of the Navy Advisory Board. He lives in New York City and is a member of the Council on Foreign Relations, and is fluent in Spanish and Italian. Devine's book, "Good Hunting! An American Spymaster's Story," a

New York Times bestseller, was published in June 2014. It chronicles his career at the Agency and the role of covert operations in the past and future.

The TAG team brings together experts from top US universities and graduate programs and has experience working in key US government agencies, international organizations, and leading consulting firms. In its activities, PIC relies on extensive national and international networks of regional and functional experts, including intelligence specialists, law enforcement officials, diplomats and politicians, industrial, business and financial analysts, leading scientists, journalists, and specialized experts in forensic science and security. TAG's specializations include business analytics, independent company verification, forensic investigations, strategic crisis consulting, political risk analysis, security, and preparedness. PIC's mission is to use strategic intelligence and predictive analysis to enable clients to minimize risk and maximize returns when making important business decisions. It has completed hundreds of assignments in every region of the globe. TAG is distinguished by its personalized approach and services. For each assignment, PIC creates a unique game plan to achieve the client's specific goals. Although it relies on a wide range of investigative, forensic, communications, and security tools, the hallmarks of TAG's methodology are sound analysis and well-sourced human intelligence. In February 2009, another American PIC appeared – The Chertoff Group [28]. It is a specialized consulting company that is a global leader in security and risk management. Its founders and key employees are former high-ranking US officials: Michael Chertoff, Secretary of Homeland Security (2005–2009); Michael Vincent Hayden, four-star general, Director of the National Security Agency (NSA) (1999–2005), Deputy Director of National Intelligence (2005–2006), Director of the CIA (2006–2009); Chad Sweet, Chief of Staff, Department of Homeland Security (2005–2009), former CIA employee; Charles Allen, Under Secretary of Homeland Security for Intelligence and Analysis (2005–2009), former Assistant Director of the CIA; Jay Cohen, Rear Admiral, Under Secretary of Homeland Security for Science and Technology (2006–2009). The Chertoff Group's team of recognized experts with

diverse experience in security in the private and public sectors helps organizations manage cyber, physical, regulatory, and geopolitical risks. Through its business development practice, it helps its clients gain competitive advantage and accelerate growth.

The Chertoff Group includes:

- Chertoff Capital, an investment banking subsidiary that advises on mergers and acquisitions (M&A) for companies in the defense technology, public services, and cybersecurity markets.
- Merchant Banking Practice, which has a proven track record of advising on nearly $8 billion in closed M&A transactions, provides integrated investment banking services and capital investments to fast-growing, mission-driven companies in the fields of national security, cybersecurity, and more.
- MC2 Investment Management, LLC, a subsidiary that provides growth capital through the MC2 Security Fund, a private equity fund that invests in the equity of rapidly growing, high-potential companies in the cybersecurity, national security, defense technology, and public services sectors. The MC2 Security Fund invests directly or through special purpose companies such as MC2 Titanium, LLC.

The Chertoff Group serves Fortune 500 companies across a range of sectors, as well as small and medium-sized businesses with specialized needs. PIC's experts and specialists base their work on anticipating what will happen next, applying best practices, and demonstrating value. Its experienced team helps organizations manage cyber, physical, transportation, and geopolitical risks; develop resilience; navigate changing regulatory and compliance requirements; and unlock opportunities to do business and create value.

The Chertoff Group is one of the few professional services firms in the world to receive the SAFETY Act designation under the U.S. Department of Homeland Security's Security Risk Management Consulting Methodology. It has developed its own methodology to enable organizations to assess, mitigate, and control physical and cyber security risks to their people, facilities, and technology assets, as well as to the business operations they support.

The Chertoff Group's mission is to apply its expertise in security, technology, and policy to help clients build resilient organizations, gain a competitive advantage, and accelerate growth. To do this, it has the following capabilities:

- 360-degree view of security risks:
- Global security risk environment;
- Business markets and investment opportunities for security and safety technologies;
- Political and regulatory interactions;
- Integrated full lifecycle advisory model:
- Security risk management;
- Organic and inorganic growth strategies;
- Transaction liquidity events;
- Equity investments.

The Chertoff Group's competitive advantages include: proven security risk management consulting methodology; demonstrated success in reducing overall security risk; enabling clients to measure and report on the effectiveness of their risk management programs; a pragmatic approach based on the experience of security operators and policy makers; the ability to translate security knowledge into value creation for clients; a strong global network of strategic relationships and trusted partners; and access to significant growth capital and investor syndicates.

Since the use of PIC in US intelligence activities had some side effects, an expert discussion was held at the National Press Club in August 2009, during which participants discussed this issue with the leaders of The Chertoff Group and The Arkin Group.

The experts were primarily interested in answers to two questions: does such privatization threaten national security interests and the future of the intelligence community? And what about the problem of "poaching" a significant number of intelligence personnel by private firms, where they use their professional knowledge and skills? During the discussion, data was presented showing that US intelligence services are outsourcing some of their traditional functions to "contractors," whose services come at a high cost. In particular, this accounts

for more than 30% of the CIA's annual budget. In addition, PICs have poached two-thirds of the senior staff of the Department of Homeland Security, who have extensive contacts in various circles, significant professional experience, and knowledge of how government agencies work.

Particularly heated discussions revolved around the issue of secret CIA programs, under which, for example, Blackwater USA (since January 2010 – Academi) received a contract in 2004 for the physical elimination of Al-Qaeda leaders. According to US media reports, the aim of this move was to shield CIA employees from possible criminal liability in the event of the operation's failure or other unforeseen circumstances.

The participants in the discussion concluded that the actions of "contractors" hired by federal agencies must comply with the same strict moral and legal standards as the actions of IC employees. The decisive factor when hiring PICs or individuals is their unique qualifications or skills, which can take a long time to acquire. In addition, "contractors" are usually called upon when there is a temporary need for knowledge and skills in a particular area. In these cases, hiring specialists saves time and resources, since "contractors" are not permanent employees and can be easily replaced if necessary. This is especially true when lawmakers set tasks for the intelligence community that require significant expenditures, but at the same time cut the budget.

As noted by J. Devine, head of The Arkin Group, in the late 1990s, Congress cut the CIA's budget by 25%. This meant that at the time of the September 11, 2001, terrorist attacks, the human and material resources of this intelligence agency were insufficient to perform its functions quickly and effectively. To solve the problem, the leadership resorted to the mass use of "contractors." However, not all functions were transferred to them; accordingly, the CIA developed task concepts and managed and controlled their implementation. At the same time, J. Devine denied that American intelligence practiced hiring PICs to eliminate terrorists (at least during his 32 years of service at the CIA).

General M. Hayden (The Chertoff Group) called for no distinction to be made between government agencies and private businesses, a significant proportion of which are willing to take risks without financial reward in order to help ensure national security. He also stressed that the lack of comprehensive data on individuals and companies working under government contracts in the field of intelligence and security is due to the need to protect sources of information. This approach should be understood, in particular, by media representatives who are showing increased interest in this issue.

The UK is currently the leader in providing private intelligence services on the European continent. According to experts, a few years ago, the budget of PICs located in London alone was close to $20 billion. It is worth describing the work of some well-known PICs operating in the UK.

SCL Group (Strategic Communication Laboratories) is a private British behavioral research and strategic communications company that was registered with Companies House on July 20, 2005, by Nigel Oakes, who was its CEO [29]. The company positioned itself as a "global election management agency." The company's managers and owners had close ties to the Conservative Party, the British royal family, the British military, the US Department of Defense, and NATO, and its investors included some of the Conservative Party's biggest sponsors.

In 1990, Nigel Oakes, who had experience in television production and advertising, founded the Behavioral Dynamics Institute (BDI) as a research center for strategic communication [30]. Oakes believed that academic ideas developed by psychologists and anthropologists at the BDI should be used to change public opinion, and that this would be more successful than traditional advertising methods. The study of mass behavior and how to change it led to the creation of Strategic Communication Laboratories, and BDI became its non-profit affiliate, SCL Group. Among the investors in SCL Group was banker Paul David Ashburner Nix, whose son Alexander Nix would become a close associate of Oakes. One of the former directors is Lord Ivar Mountbatten. Among the company's investors

were Jonathan Marland, Baron Marland, and Roger Gabb, a major Conservative Party donor who was registered as having significant control over the company as of 2018.

After its initial commercial success, SCL Group expanded its presence in the military and political arenas. It became known for its alleged involvement in military disinformation campaigns involving social media branding and voter targeting. SCL Group began to focus on elections in developing countries, engaging with their military and politicians to study and manipulate public opinion and political will. To do this, the PIC used what were called "psychological operations" to gain insight into the thinking of the target audience. It conducted an intellectual analysis of data and analysis of data about its audience. Based on the results, it targeted communications specifically at key audience groups to change behavior in line with its clients' requirements. In the early 1990s, the PIC was involved in psychological warfare in military contexts as a contractor for the US and British military during the wars in Afghanistan and Iraq.

In 2005, at the Defence and Security Equipment International (DSEI) exhibition, the largest military technology exhibition in the United Kingdom, SCL Group demonstrated its capabilities in "influence operations," showing how it could help organize a complex campaign of mass deception of the public in a city as large as London. SCL Group claims that its methodology has been endorsed by, among others, agencies of the UK government and the US federal government.

According to information on its website, since 1994, SCL Group has participated in more than 25 international political and election campaigns and has influenced elections in Italy, Latvia, Ukraine, Albania, Romania, South Africa, Nigeria, Kenya, Mauritius, India, Indonesia, the Philippines, Thailand, Taiwan, Colombia, Antigua, Saint Vincent and the Grenadines, Saint Kitts and Nevis, and Trinidad and Tobago.

In 2013, SCL Group founded a subsidiary, Cambridge Analytica (CA), which specializes in providing consulting services in the political sphere, using deep data analysis technologies, in particular those

from social media, to develop strategic communication on the Internet during election campaigns [31]. These technologies are based on algorithms developed by Cambridge University employee Michal Kosinski, which allow the creation of psychological profiles of web resource users. This PIC was created to participate in the electoral process in the United States and participated in 44 elections to the US Congress, US Senate, and state-level elections in the 2014 midterm elections. In 2015, the company participated in the Republican Party's presidential primaries for the 2016 election, mainly in support of Ted Cruz.

CA was largely funded by billionaire hedge fund manager Robert Mercer, a major supporter of Cruz and then Donald Trump. According to The Guardian, Cambridge Analytica formed a global network of sources, "taking root" in 68 countries around the world.

It is believed that Cambridge Analytica helped the government convince the UK population to vote in favor of leaving the EU in the 2016 referendum. A few years later, the UK Parliament Intelligence and Security Committee (ISC) published its Russia Report, which mentioned possible Russian interference in the Brexit referendum. Cambridge Analytica was also mentioned in the investigation. It is worth noting that in 2017, Russia's Sberbank used the company's services to improve its system for assessing the creditworthiness (credit risks) of its customers.

In 2018, Cambridge Analytica found itself at the center of an international scandal: it came to light that the company had illegally accessed the data of 87 million Facebook users while working on US President Donald Trump's election campaign. In addition, the British television broadcaster Channel 4 released recordings of conversations with the PIC's managers, from which it can be concluded that Cambridge Analytica employees resort to bribes to discredit politicians. The scandal led to Facebook blocking Cambridge Analytica's access to all of its services, and the company itself came under investigation by the British and US governments. Since then, the company has been disbanded and bought by Emerdata Limited. In 2019, the Federal Trade Commission (FTC) filed an administrative complaint

against Cambridge Analytica for misuse of data, while simultaneously entering into settlement agreements with its former CEO, Alexander Nix, and app developer Aleksandr Kogan, in which they agreed to delete the illegally obtained data.

In 2020, Alexander Nix signed a disqualification agreement approved by Alok Sharma, Secretary of State for Business, Energy and Industrial Strategy, on September 14, 2020. Effective October 5, 2020, Alexander Nix is disqualified for seven years from acting as a director or directly or indirectly participating, without court permission, in the promotion, incorporation, or management of a UK company.

PIC Emerdata Limited was founded in August 2017 by a group of people associated with Cambridge Analytica: the data director and head of Cambridge Analytica's parent company, SCL Group, which ceased operations on May 1, 2018 [32]. Its London headquarters are located in the same building as Cambridge Analytica. It has been reported that the company offers similar services to those of SCL Group and Cambridge Analytica.

Emerdata's board of directors includes Frontier Services Group employee Johnson Chun Shun Ko, a Hong Kong businessman associated with Erik Prince (founder of Blackwater), Cambridge Analytica investor Rebekah Mercer, and Cambridge Analytica CEO Alexander Nix. In January 2018, Emerdata Limited raised $19 million from international investors and was widely discussed in the media. It was portrayed as a potential successor to Cambridge Analytica. In May 2018, Nigel Oakes, founder of SCL Group, the British affiliate of Cambridge Analytica, acknowledged that Emerdata intended to acquire Cambridge Analytica and SCL, but said that these plans had been abandoned and that Emerdata and its stake in Firecrest Technologies Ltd, a subsidiary created by former Cambridge Analytica CEO Alexander Nix, would be liquidated.

In July 2019, it emerged that Emerdata had made a full acquisition of these companies, paid SCL's legal bills amid bankruptcy proceedings, investigations, and lawsuits on both sides of the Atlantic, and paid millions to acquire what remained of the companies while they were in the process of being liquidated.

In the context of the study, the activities of several Israeli PICs are of interest. Psy-Group was founded in 2014 by Roy Burstein, a former lieutenant colonel in the Israeli army who headed a special intelligence unit within the country's government and later became the CEO of this PIC [33]. The owner was Joel Zamel, an Australian Jew who made his fortune in mineral extraction. Among the advisors were former Mossad deputy director Ram Ben-Barak and Yaakov Amidror, former head of the National Security Council in Benjamin Netanyahu's office. The company's legal advisor was Daniel Reisner.

Psy-Group was involved in managing online image, influence/manipulation campaigns on social media, opposition research, honeytraps, and covert field operations for clients. Psy-Group was sometimes referred to as the "private Mossad."

In 2016, the PIC launched Project Butterfly, designed to combat the BDS movement on American university campuses. Psy-Group offered its sponsors the opportunity to undermine the stability of organizations promoting the boycott of Israel from within. The company's employees searched social networks and publicly available sources, as well as the so-called Dark Web, for information that could discredit BDS activists or sow discord within BDS groups.

As an example, The New Yorker journalists cite the publication of photographs of Muslims drinking alcohol or replacing their wives. The results of Psy-Group's work were always published in such a way that they could not be linked to either the company or its clients. According to The New Yorker, a total of $2.5 million was invested in the project, and the fight against the BDS movement spread to 10 major American universities.

Psy-Group was financially linked to the Metropol Group, headed by Russian millionaire Mikhail Slipenchuk, a former member of the Russian State Duma from the United Russia party. At one time, Psy-Group provided services to Russian oligarchs Oleg Deripaska and Dmitry Rybolovlev, Deputy Head of the General Intelligence Service of Saudi Arabia Major General Ahmad Asiri (involved in the murder of journalist Jamal Khashoggi), and the corrupt president of Gabon, Ali Bongo Ondimba. In addition, in June 2016, Joel Zamel participated in

the St. Petersburg International Economic Forum, which was held with the participation of the Russian president.

In 2016, this PIC collaborated with the British company Cambridge Analytica during the election campaign of US President Donald Trump. Joel Zamel met with Donald Trump Jr. and Jared Kushner, offering them to launch an online campaign to destroy the political reputation of Trump's rivals (Psy-Group employees carried out such an operation at least once on the eve of parliamentary elections in one of the European countries). The campaign used the following methods: infiltrating the target audience on social media with specially created fake accounts; spreading misleading information through websites that imitated news portals; discrediting political opponents by organizing bribery or accusations of sexual harassment. Psy-Group's activities later became part of an investigation by the FBI and the Senate Select Committee on Intelligence into possible Russian interference in the US presidential election.

In 2017, PIC conducted a disinformation campaign against the Ukrainian Anti-Corruption Action Center (AntAC), targeting its chairman, Vitaliy Shabunin, and its executive director, Daria Kaleniuk. The Psy-Group's campaign to discredit AntAC members resulted in at least two YouTube videos spreading false information about Ukrainian activists. Two completely fake "English-language news reports" were posted on the Storozh Ukraina channel and have over 20,000 views, indicating that the videos were promoted through advertising. Storozh Ukraina is another anonymous association of citizens who "expose" anti-corruption activists. In March 2017, senior Saudi Arabian officials close to Crown Prince Mohammed bin Salman offered several PICs $2 billion to organize a series of contract killings. In particular, they were interested in the commander of the Quds Force unit of Iran's Islamic Revolutionary Guard Corps, General Qasem Soleimani.

The meeting was attended by the aforementioned deputy head of Saudi Arabia's General Intelligence Service, Major General Ahmad Asiri, and Joel Zamel, who allegedly refused the offer. However, it should be noted that Qasem Soleimani was killed on January 3, 2020,

in a targeted airstrike by the US Air Force. According to some reports, information about the general's whereabouts was provided to the American side by the Mossad.

In 2018, after Special Counsel Robert Mueller's commission took an interest in Psy-Group's activities, Joel Zamel was forced to shut it down, and some of its employees moved to Black Cube, a company involved in the Harvey Weinstein case and in gathering compromising information on Barack Obama. Joel Zamel himself remains the head of the Zamel Group, which includes the US-based PIC Wikistrat, founded in 2010 [34]. From 2014 to 2017, its director of strategic development was former Israeli intelligence officer Shay Hershkovitz. Wikistrat's line of business involves geostrategic consulting using crowdsourcing (engaging a wide range of individuals to utilize their creative abilities, knowledge, and experience for something like subcontracting on a voluntary basis using information technology).

PIC White Knight Group, which is essentially the successor to Psy-Group, was founded in 2017 [35]. This PIC specializes in social media campaigns, influence operations, and election campaign management. The group is also an active investor in transnational infrastructure projects, including AI development and the cybersecurity sector, especially for companies in Central and Eastern Europe. Methods similar to those used by Psy-Group: online image management, influence through social media, manipulative campaigns, strategic disinformation (e.g., production of fake news or propaganda), political campaigns using social media and AI. The same tactics are used by other Israeli PICs – Archimedes Group and Black Cube [36, 37].

The tactics of Archimedes Group, which targets a number of African countries, Latin America, and Southeast Asia, are very similar to the information warfare tactics often used by the governments of certain countries, particularly Russia. For its part, Black Cube eavesdropped on non-governmental organizations in Hungary on the eve of the spring 2018 election campaign in order to gather compromising information to pass on to the headquarters of the country's Prime Minister Viktor Orbán.

Some PICs specialize in providing technical support for intelligence activities. One of them is the Israeli-American Verint Systems Inc., which was founded in 1994 and has an estimated 5,000–10,000 employees [38]. In 2017, it acquired a small PIC, Terrogence, founded in 2005 by former Shin Bet counterintelligence officer Shai Arbel [39]. Both companies actively contract with the US government to provide the NSA and other intelligence agencies with the latest espionage technologies. Among these technologies is the Face-Int service, designed for facial recognition, based on a database of many thousands of individuals suspected of illegal activity. Terrogence actively tracked and collected information on the Internet about terrorists and other individuals who posed a threat to national security (particularly in the areas of air transport security, immigration, etc.). The sources of such data were YouTube, Facebook, and various open and closed forums. In April 2018, information about the Face-Int service disappeared from the Terrogence website, but it can be assumed that the company continues to provide such services and uses more sources of information than was officially known. The exact technology used by the Face-Int service to obtain facial images remains unknown, but the description of the program resembles one of the US National Security Agency (NSA) projects exposed by Edward Snowden in 2014. During the three years of the project's existence, this special service collected 55,000 high-quality images of identified faces. It appears that Terrogence is violating Facebook's policy, which prohibits the use of data obtained from the social network to track users. The use of any automated methods of collecting information, such as bots, is also prohibited.

There is no evidence that the US government may be using the Face-Int service, but open data shows that Terrogence has at least two government contracts with the US Navy totaling nearly $150,000. This amount is equivalent to an annual subscription to two services of this PIC – Mobius and TGAlertS. The Mobius service is a collection of materials from various social networks and platforms on the latest trends in explosive devices created by terrorists and methods of their use, while TGAlertS contains operational information on some important events obtained by Terrogence employees from the Internet.

Although Terrogence's main focus is working with intelligence and law enforcement agencies to combat terrorism, the LinkedIn profiles of former employees mention "working with public opinion for government clients" and using "social media methods to study political and social groups."

Another area of activity of PICs, similar to Terrogence, that is causing public concern is the creation of various "blacklists." In 2018, Verint launched another facial recognition program, FaceDetect, which enables the identification of individuals regardless of their ethnicity, any obstacles, aging, or concealment, and instantly adds data to a registry of wanted persons. The main problem with such registries created by states is the algorithm for including specific individuals in them and the scope of application of the collected data.

In February 2021, Amnesty International reported that Verint Systems had provided the South Sudanese National Security Service with equipment for intercepting communication channels. This special service is accused of persecuting, intimidating, arbitrarily detaining, and, in some cases, forcibly disappearing and even killing political opponents of the regime.

The United Arab Emirates (UAE) also has its own PIC, DarkMatter Group (DarkMatter), which was founded in 2014 by Emirati businessman Faisal Al Bannai, founder of mobile phone supplier Axiom Telecom and son of the Major General of the Dubai Police [40]. This PIC positioned itself as a computer security company engaged exclusively in defensive measures, but some experts claim that DarkMatter is involved in "offensive" measures, i.e., hacking computer networks, cyber attacks, and illegally accessing data on the Internet, particularly in the interests of the UAE government. In the same year, 2014, DarkMatter's subsidiary, Zeline 1, began operations in Finland. It recruited former NSA employees and officers from the technical divisions of the Israel Defense Forces, offering them up to $1 million per year.

DarkMatter made its public debut in 2015 at the 2nd Annual Arab Future Cities Summit. At the time, the company promoted capabilities such as network security and troubleshooting, promised to

create a new "secure" mobile phone, and positioned itself as a "digital defense and intelligence service" for the UAE.

In 2016, reports emerged that CyberPoint, which worked for the UAE government, had signed a contract with the Italian company Hacking Team, a spyware developer, which undermined CyberPoint's reputation as a cybersecurity firm. The UAE, dissatisfied with relying on an American contractor, replaced CyberPoint with DarkMatter, which became the contractor for Project Raven instead of CyberPoint. This project was a confidential initiative designed to help the UAE government monitor terrorists, political opponents, and foreign governments. Its team included former US intelligence agents who used their training to hack into the phones and computers of Raven project targets. The operation was conducted in a converted mansion in the Abu Dhabi suburb of Khalifa City, known as "The Villa." Project Raven originated in 2008 as the Development Research Exploitation and Analysis Department (DREAD), created by Richard Clarke through his security consulting group Good Harbor Consulting as a division of the UAE royal court of Mohamed bin Zayed Al Nahyan. By the end of 2010, Good Harbor had divested itself of DREAD, ceding control to Karl Gumtow, co-founder and CEO of CyberPoint. From 2014 to 2016, CyberPoint provided US-trained contractors to Project Raven. After that, the Raven project expanded its surveillance to include Americans, potentially involving its American employees in illegal activities. For example, DarkMatter hacked into emails between First Lady Michelle Obama and a former Qatari minister about Michelle Obama and Conan O'Brien's trip to Qatar in November 2015. Obama and O'Brien visited Al Udeid Air Base, which houses the forward headquarters of US Central Command and the Royal Air Force's 83rd Expeditionary Air Wing. The air base also served as the headquarters of the US Air Force Central Command during the wars in Iraq and Afghanistan. DarkMatter was very interested in hacking into Qatar's computers to obtain and read its electronic communications, as Qatar was believed to support the Muslim Brotherhood. After The Intercept published an article on October 24, 2016, exposing DarkMatter's surveillance, Samer Khalife, DarkMat-

ter's CFO, transferred some US citizens from DarkMatter to a new company called Connection Systems.

That same year, Project Raven purchased a tool called Karma. Karma could remotely hijack an Apple iPhone anywhere in the world without any interaction from the iPhone owner, as long as the user's name, such as their Apple ID, email address associated with the phone, or phone number, was provided. Raven operatives could view passwords, emails, text messages, photos, and location data from a compromised iPhone. Among those whose cell phones were deliberately hacked using Karma were the Emir of Qatar, Sheikh Tamim bin Hamad bin Khalifa Al Thani, as well as his brother and several other close associates; Nadia Mansoor, wife of imprisoned UAE human rights activist Ahmed Mansoor; British journalist Rori Donaghy; Lebanese Prime Minister Saad Hariri; Yemeni Nobel Prize winner Tawakkol Karman (leader of the Arab Spring); hundreds of other iPhone users in Europe and the Middle East, including the governments of Qatar, Yemen, Kuwait, Oman, Serbia, Lebanon, Iran, and Turkey.

Also in 2016, DarkMatter sought out smartphone development experts in Oulu, Finland, and hired several Finnish engineers. It developed a smartphone model called Katim, which translates from Arabic as "silence." In 2021, DarkMatter's cyber operations were transferred to Digital14, headquartered in Abu Dhabi, which distributed the secure Katim communication system. Digital 14 positions itself as one of the leading cybersecurity companies in the Middle East, serving customers in the government, energy, transportation, financial, and healthcare sectors.

In early 2018, DarkMatter's turnover was in the hundreds of millions of dollars. It is known that 80% of PIC's contracts are with UAE government agencies, including the Radio Intelligence Agency (RIA), formerly known as the National Electronic Security Authority (NESA). This special service is the UAE's intelligence agency, similar to the NSA, which was created in 2011 with the help of the US in response to possible cyber espionage by Iran.

In 2018, Faisal Al Bannai confirmed that DarkMatter worked very closely with the UAE government and was a competitor to the

Israeli company NSO Group. From January 2016 to November 2019, thanks to its experts — former NSA employee Marc Baier, as well as Ryan Adams and Daniel Gericke, who worked in US military and intelligence circles — DarkMatter significantly improved the services it provided to the UAE government.

In January 2020, based on the FBI's investigation, particularly regarding DarkMatter, for crimes such as digital espionage services, involvement in the murder of Jamal Khashoggi, and the imprisonment of foreign dissidents, the US Congress passed a bill proposed in 2019 by Congressman Max Rose of New York. The law requires the IC to annually assess threats to national security that may arise from the activities of former intelligence officers who, after leaving the service, work for foreign companies, organizations, and governments.

In 2021, Loujain al-Hathloul filed a lawsuit in the U.S. District Court in Oregon against three former US intelligence and military officers who conducted hacking operations on behalf of the UAE. According to the lawsuit, the three men — Marc Baier, Ryan Adams, and Daniel Gericke — worked for DarkMatter and helped Emirati security officials extract data from her iPhone. The hack led to al-Hathloul's arrest in the UAE and extradition to Saudi Arabia, where she was detained, imprisoned, and tortured.

On September 14, 2021, Marc Baier, Ryan Adams, and Daniel Gericke were charged with violating US laws related to computer fraud and the improper export of technology. They agreed to deferred prosecution in exchange for: paying fines of $750,000, $600,000, and $335,000 over three years, respectively, for a total of $1.68 million; assisting the FBI and Department of Justice in their investigations; termination of ties with any UAE intelligence and law enforcement agencies; compliance with a ban on services, including defense articles subject to the International Traffic in Arms Regulations (ITAR), and future work involving the operation of computer networks; renouncing their security clearances in the US and any foreign organization; accepting a lifetime ban on future security clearances in the US.

In December 2021, US lawmakers called on the Treasury Department and the State Department to impose sanctions on DarkMat-

ter, NSO Group, Nexa Technologies, and Trovicor. A letter signed by Senate Finance Committee Chairman Ron Wyden, House Permanent Select Committee on Intelligence Chairman Adam Schiff, and 16 other lawmakers requested the imposition of global Magnitsky sanctions, as the companies were accused of contributing to human rights violations.

In conclusion, it can be said that it is strategically important for any state to be aware of events and processes that take place outside its borders but may be of interest for developing tactics and building strategies for an appropriate response. The activities of PICs are significant from this point of view. PICs often outpace special services in the creation and application of the latest technologies in their activities. These organizations not only carry out orders from government agencies, but are also targets of intelligence interest for other countries seeking to obtain the information they possess. PICs can be used for political struggle. Therefore, their activities must be controlled by the state through specialized legislation. Ukraine should study foreign experience in the functioning of PICs and use it to strengthen its national security.

Conclusions to Section IV

An analysis of recent events indicates a transformation in views on the tasks and functioning of intelligence.

The key advantages of breakthrough technological innovations in intelligence activities are as follows:

UAVs and satellites, which provide effective and economical real-time monitoring, reducing risks to military personnel;

New developments in sensor technology that expand the capabilities of intelligence gathering to detect, identify, and track potential threats.

Ground-based surveillance radars with built-in advanced signal processing algorithms that enable the detection of personnel and vehicle movements over long distances, providing early warning systems.

The use of AI algorithms which make it possible to process large amounts of data collected by surveillance systems, identifying patterns and anomalies that analysts may miss.

The use of machine learning algorithms, which enable the automatic detection and classification of threats, helping the armed forces to respond effectively to the situation.

Conducting big data analysis to obtain valuable information from monitoring observations, enabling optimal decisions to be made and future military operations to be planned.

Analytical discourses and direct intelligence practices in Western countries suggest that modern intelligence is conceived as a complex, multidisciplinary, science-intensive process that requires constant transformation of "intelligence pedagogy" in order to train effective – multi-profile – specialists who are psychologically and physically resilient, academically and professionally capable of collecting, understanding, integrating, and transmitting data from multiple sources, as well as conducting strategic intelligence, forecasting (taking into account future challenges), relying on the capabilities of AI, etc.

The provisions of the White Paper for European Defence – Readiness 2030 indicate that the EU, given Russia's invasions of other countries and its current policy of expansion, perceives Russia as an "existential threat to the European Union". Changes in US approaches to European security are identified as a reality that must be taken into account, but NATO remains the cornerstone of collective defense. The general political balance that had been established after the end of World War II has been "irreversibly disrupted." The formation of a new world order is a new reality that will emerge in the short term, and Europe must become an active participant in its creation rather than a passive "consumer of consequences."

A study of public-private partnerships in the field of intelligence activities, using the example of the most famous PICs in the US, the UK, Israel, and the UAE, showed that they act as contractors for state structures as collectors and processors of intelligence information, with the help of which the state learns about its external environment

and realizes its own tasks in this area. PICs can also be used for political struggle, so their activities must be controlled by the state on the basis of specially created legislation.

References:

1. Kresina, I. O. (Ed.). (2024). *Stratehichni priorytety polityko-pravovoho rozvytku Ukrainy v konteksti yevropeiskoi intehratsii: monohrafiia* [Strategic priorities of political and legal development of Ukraine in the context of European integration: Monograph]. Norma Prava.
2. Mykhalchenko, M. (2011). Interesy natsionalni [National interests]. In Yu. Levenets & Yu. Shapoval (Eds.), *Politychna entsyklopediia* [Political encyclopedia] (p. 808). Parlamentske Vydavnytstvo.
3. Verkhovna Rada of Ukraine. (2003, June 19). *Pro osnovy natsionalnoi bezpeky Ukrainy: Zakon Ukrainy No. 964-XV* [On the principles of national security of Ukraine: Law of Ukraine No. 964-XV]. https://zakon.rada.gov.ua/laws/show/964-15#Text
4. Sytnyk, H. (Ed.). (2016). *Hlobalna ta natsionalna bezpeka* [Global and national security]. NADU.
5. Reznikova, O., & Smolianiuk, V. (2023). Conceptual Issues of National Security Policy-Making Under Uncertainty. *Politologija*, *111*(3), 41-73. https://doi.org/10.15388/Polit.2023.111.2
6. Krutii, V. O. (2018). *Transformatsiia politychnoi systemy suspilstva v umovakh hibrydnoi viiny* [Transformation of the political system of society in conditions of hybrid war] (Doctoral dissertation abstract). V. M. Koretsky Institute of State and Law of the National Academy of Sciences of Ukraine.
7. Tsymbal, I. V., Zhovtun, A. A., & Limanska, O. L. (2015). Svit VUCA yak suchasnyi kontekst informatsiinykh i suspilno-politychnykh zmin [VUCA world as a modern context of information and socio-political changes]. *Naukovyi chasopys Natsionalnoho pedahohichnoho universytetu imeni M. P. Drahomanova. Seriia 22: Politychni nauky ta metodyka vykladannia sotsialno-politychnykh dystsyplin*, *(17)*, 43–47.

8. Dohadailo, Ya. V., & Laptieva, U. D. (2021, May 28). Peredumovy vyzhyvannia u VUCA-sviti [Prerequisites for survival in the VUCA world]. In *Oblikovo-analitychnyi ta ekonomiko-finansovyi instrumentarii upravlinnia suchasnym pidpryiemstvom: mizhnarodnyi dosvid: materialy mizhnar. nauk.-prakt. konf.* [Accounting, analytical, economic and financial tools for modern enterprise management: international experience: proceedings of the international scientific and practical conference] (pp. 126–130). Kharkiv National Automobile and Highway University. https://dspace.khadi.kharkov.ua/handle/123456789/17603

9. Mokliak, S. P. (Ed.). (2025). *Shtuchnyi intelekt yak chynnyk zabezpechennia natsionalnoi bezpeky: monohrafiia* [Artificial intelligence as a factor in ensuring national security: Monograph]. Bykhun V. Yu.

10. Burns, W. J. (2023, July 1). *A world transformed and the role of intelligence* [Speech transcript]. Ditchley Annual Lecture, Ditchley Park. Central Intelligence Agency. https://www.cia.gov/static/62739354dfed5cc1942997d3f1899d94/DCIA-Ditchley-Remarks-01-July-2023.pdf

11. Burns, W. J. (2024, January 30). *Spycraft and statecraft: Transforming the CIA for an age of competition*. Foreign Affairs. https://www.foreignaffairs.com/united-states/cia-spycraft-and-statecraft-william-burns

12. Office of the Director of National Intelligence. (2025, March 25). *2025 annual threat assessment of the U.S. intelligence community.* https://www.dni.gov/files/ODNI/documents/assessments/ATA-2025-UnclassifiedReport.pdf

13. European Commission, & High Representative of the Union for Foreign Affairs and Security Policy. (2025). *Joint White Paper for European Defence Readiness 2030* (52025JC0120). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52025JC0120

14. North Atlantic Treaty Organization. (2025). *NATO warfighting capstone concept.* https://www.act.nato.int/our-work/nato-warfighting-capstone-concept/(Accessed May 20, 2025)

15. Vinci, A. (2020, August 31). The coming revolution in intelligence affairs: How artificial intelligence and autonomous systems

will transform espionage. *Foreign Affairs.* https://www.foreignaffairs.com/articles/north-america/2020-08-31/coming-revolution-intelligence-affairs

16. Stenslie, S., Haugom, L., & Vaage, B. H. (2021). *Intelligence analysis in the digital age (1st ed.).* Routledge. https://doi.org/10.4324/9781003168157

17. Hammond-Errey, M. (2024). *Big data, emerging technologies and intelligence: National security disrupted (1st ed.).* Routledge. https://doi.org/10.4324/9781003389651

18. Lin-Greenberg, E., & Milonopoulos, T. (2021, September 23). Private eyes in the sky: How commercial satellites are transforming intelligence. Foreign Affairs. https://www.foreignaffairs.com/world/private-eyes-sky (Accessed May 20, 2025)

19. Zegart, A., & Morell, M. (2019, April 16). Spies, lies, and algorithms: Why U.S. intelligence agencies must adapt or fail. Foreign Affairs, 98(3). https://www.foreignaffairs.com/united-states/spies-lies-and-algorithms

20. Haines, A. D. (2023, August 15). National Intelligence Strategy 2023 (Technical Report No. AD1208004, 20 pp.). Office of the Director of National Intelligence. https://apps.dtic.mil/sti/html/trecms/AD1208004/index.html

21. Palyvoda, V. O. (2022). Pryvatni rozviduvalni kompanii: inozemnyi dosvid zaluchennia pryvatnoho sektoru do vykonannia zavdan rozvidky [Private intelligence companies: Foreign experience of engaging the private sector in intelligence tasks] (Analytical report, 20 pp.). Kyiv: National Institute for Strategic Studies. https://doi.org/10.53679/NISS-analytrep.2022.06

22. Semeniuk, Y. V., & Lysetskyi, Y. M. (2025). Derzhavno-pryvatne partnerstvo u sferi natsionalnoi bezpeky [Public-private partnership in the field of national security]. *Derzhava i pravo*, (97), 118–146.

23. DSS BI Analytics+. (2019, January 15). *Pohliad z Ukrainy na amerykansku korporatsiiu "soldativ rozumu" RAND Corporation* [A view from Ukraine on the American corporation of "soldiers of

reason" RAND Corporation]. https://dss-bi.blogspot.com/2019/01/rand-corporation.html (Accessed May 20, 2025)

24. Strategic Forecasting Inc. https://stratfor.com/ (Accessed May 25, 2025)

25. Geopolitical Futures (GPF). https://geopoliticalfutures.com/welcome/ (Accessed May 25, 2025)

26. The Arkin Group. https://thearkingroup.com/ (Accessed May 27, 2025)

27. The Chertoff Group. https://thearkingroup.com/ (Accessed May 27, 2025)

28. Strategic Communication Laboratories. https://www.devex.com/organizations/strategic-communication-laboratories-41754 (Accessed May 29, 2025)

29. Behavioral Dynamics Institute. https://behavioraldynamic-sinc.com/ (Accessed May 29, 2025)

30. Cambridge Analytica. (2024, May 12). In Wikipedia. Retrieved June 5, 2025, from https://en.wikipedia.org/wiki/Cambridge_Analytica

31. Emerdata Limited. (n.d.). In Wikipedia. Retrieved June 6, 2025, from https://en.wikipedia.org/wiki/Emerdata_Limited

32. Psy-Group. (n.d.). In Wikipedia. Retrieved June 8, 2025, from https://en.wikipedia.org/wiki/Psy-Group

33. Wikistrat. (n.d.). In Wikipedia. Retrieved June 10, 2025, from https://en.wikipedia.org/wiki/Wikistrat

34. White Knight Group. https://www.whiteknightgroup.com/ (Accessed June 12, 2025)

35. Archimedes Group. (n.d.). In Wikipedia. Retrieved June 14, 2025, from https://en.wikipedia.org/wiki/Archimedes_Group

36. Black Cube. https://www.blackcube.com/ (Accessed June 16, 2025)

37. Verint Systems Inc. (n.d.). In Wikipedia. Retrieved June 18, 2025, from https://en.wikipedia.org/wiki/Verint_Systems

38. Terrogence Ltd. (n.d.). *Bloomberg* https://www.bloomberg.com/profile/company/1251707D:IT (Accessed June 20, 2025)

39. DarkMatter Group. (n.d.). In Wikipedia. Retrieved June 20, 2025, from https://en.wikipedia.org/wiki/DarkMatter_Group

FOR NOTES

FOR NOTES

FOR NOTES

Scientific Monograph

Semeniuk Yurii Volodymyrovych, Mokliak Serhii Petrovych,
Lysetskyi Yurii Mykhailovych

THE NEW GEOMETRY OF INTERNATIONAL RELATIONS AND INTELLIGENCE ACTIVITIES

Under the general editorship of Serhii P. Mokliak

Literary editing, proofreading – Anna V. Halushkina
Print design – Viktor Y. Bykhun
Cover design – Oleh O. Starovoitenko

Signed off for printing 15.04.2026. Page size 64x90/16.
Coated paper. Offset print.
App. p. 14,45. Print run 500 copies. Зам. № 12/2
Bykhun V. Y.
9, Leontovycha str., b.18, Kyiv, 01054,
Certificate confirming the entry of a publishing entity
to the State Register of Publishers, Manufacturers and
Distributors of Publishing Products
Cert. № 5366 from 26.06.2017,
mob.: +38 050 310 22 04
e-mail: lk@ukr.net