ISSN: 2053-3578 I.F. 12.34

NEW TRENDS IN THE SECURITY OF MILITARY FACILITIES: FOREIGN EXPERIENCE IN THE INTEGRATION OF ARTIFICIAL INTELLIGENCE, DRONES, AND ADVANCED TECHNOLOGIES

Nematillayev Shuhratjon Qodirovich
Independent researcher, Colonel
University of Public Security of the Republic of Uzbekistan

Abstract: This article analyzes the military power indicators of the world's leading states—such as the United States, Russia, China, and others—based on the Global Firepower Index, and examines strategies for guarding military units, as well as the application of advanced technologies, artificial intelligence, and unmanned aerial vehicles. The paper discusses modern paradigms of military facility protection, integration among different branches of the armed forces, and mechanisms for responding to global security threats. In addition, the role of unmanned aerial vehicles and electronic warfare systems is emphasized using the example of the war in Ukraine. As a result, practical recommendations for improving national defense systems are proposed, and a theoretical and practical foundation is formed for innovative approaches to the protection of military units in the current geopolitical environment.

Keywords: military units, protection, foreign experience, Global Firepower, artificial intelligence, drones, missile defense systems, military technologies, geopolitical security.

For the world's top ten leading countries, a ranking of military power in the field of military facility protection has been formed based on the Global Firepower military strength index, as well as recent data on technological innovation and defense budgets. This list includes states with highly developed defense potential, advanced military technologies, robust defense infrastructure, and extensive military resources. These countries effectively employ modern security paradigms, automated surveillance systems, artificial intelligence–based command tools, and comprehensive cyber defense strategies to protect military facilities. At the same time, their military facility protection systems are distinguished by integration among different branches of the armed forces, high mobility, and centralized data management.

The results of this analysis provide an important scientific and practical basis for improving the protection of military facilities, strengthening national security systems, and effectively responding to international security threats. In particular, the United States leads

with a defense budget exceeding 831 billion USD and major technological achievements. It possesses the world's largest air force, with 13,209 military aircraft, including fifth-generation F-22 and F-35 fighters, unmanned combat aerial vehicles, and 11 aircraft carriers. Advanced cyber warfare systems, missile defense systems (THAAD and Aegis), and U.S. unmanned military platforms have become key components of modern military strategy.

Russia, with a defense budget of 109 billion USD and a military contingent of 3.57 million personnel, is one of the world's largest armies. Its military potential is reinforced by advanced missile systems (S-400, hypersonic Kinzhal missiles) and a nuclear arsenal. Military modernization programs are aimed at strengthening the defense of military facilities across various strategic regions.

China, with a budget of 227 billion USD and 3.17 million soldiers, has one of the world's largest armed forces. China's J-20 stealth fighter, strengthened naval fleet, anti-satellite weapons, and rapid deployment systems are directed toward reinforcing strategic military defense.

India, with the aim of ensuring regional security, is developing Arjun tanks, Tejas fighters, and Prithvi missile defense systems with a force of 5.13 million personnel and a budget of 74 billion USD. Efforts to strengthen India's domestic defense industry are shaping an independent military strategy.

The United Kingdom maintains global military influence with F-35B fighters, an advanced naval fleet, a defense budget of 62.8 billion pounds sterling, and a military contingent of 1.1 million personnel. Its leading role in NATO and the strategic placement of military bases ensure high defense capability for its units.

South Korea, with an approximate budget of 45 billion USD and a military contingent of 3.82 million personnel, is developing advanced military technologies such as the K2 Black Panther tank and the KM-SAM air defense system. Geostrategic confrontation with North Korea serves as a driving force for this development.

France, with a budget of approximately 50 billion euros and 202,761 military personnel, is increasing power projection through the Charles de Gaulle aircraft carrier, Rafale fighters, and modern drone systems. Its military strategy is aimed at strengthening Europe's security infrastructure.

Japan, with an approximate budget of 55 billion USD and more than 1,400 military aircraft, focuses its defense strategy primarily on maritime security and missile defense systems (such as Aegis), becoming a leading military power in the Asia-Pacific region.

ISSN: 2053-3578 I.F. 12.34

Israel, despite having a relatively small army and a budget of approximately 30 billion USD, ensures regional security through the Iron Dome system, Merkava tanks, and advanced drone technologies. Its high-tech defense infrastructure is aimed at increasing the military effectiveness of its units.

Germany is expanding its modern defense capabilities with Leopard 2 tanks and Eurofighter Typhoon fighters. Participation in NATO and integration of advanced technologies ensure the effectiveness of German military units. This ranking is based on a comprehensive analysis of military strength indicators, defense expenditures, and technological achievements.

According to the Global Firepower Index, the strategy for protecting military units is based on the balance and harmony between offensive and defensive technologies. Therefore, this ranking reflects the most advanced technologies and strategies for the protection of military facilities. Research conducted in the fields of military security systems such as “Force Protection,” “Base Security,” or “Military Defense Systems” is largely based on data from the Global Firepower military strength index [1].

While leading positions are occupied by the United States, Russia, and China, countries such as India, the United Kingdom, France, and Germany are supplying large quantities of weapons and military equipment to ongoing military conflicts. It has been reported that Ukraine has become the world’s largest arms importer.

According to available data, since the beginning of Russian attacks, at least 35 countries have supplied weapons to Ukraine. In the period 2020–2024, Ukraine accounted for 8.8 percent of global arms imports. The largest shares of arms supplies to Ukraine came from the United States (45%), Germany (12%), and Poland (11%). Ukraine was the only European country to enter the top ten arms importers during 2020–2024, while many other European states significantly increased their arms imports [2]. This indicates that the system of protecting military units, based on the integration of defense technologies and their direct coordination with personnel involved in protection, is a key factor in achieving high effectiveness. This, in turn, is closely linked to a country’s geopolitical position, economic capacity, socio-cultural characteristics, historical experience, and strategic objectives, as well as the size of its armed forces.

An overview of scientific research conducted in developed countries on the protection of military units shows that over the past ten years, modern military operations have proposed new trends and ideas for the use of advanced technologies in the protection of military bases. American scholar Martin C. Libicki has made a significant contribution to strengthening

cybersecurity in U.S. military systems and developing strategies for base protection, focusing on organizing defenses against cyberattacks within military units and the use of modern technologies in protecting military bases [3].

Indeed, in the United States, information systems applied in public administration and public services, defense, national security, law enforcement, the fuel and energy complex (including nuclear energy), the banking and financial system, transport, information and communication technologies, and other sectors of the economy—particularly in military security—have led to the creation of highly effective security systems.

Based on the experience of the United States and Israel, David E. Johnson studied modern approaches to the defense of military bases and proposed the use of new technologies in protection and defense, especially in safeguarding military bases in contemporary military operations [4]. Israel also holds a leading position in military base defense. In this regard, the creation of the Iron Dome system should be acknowledged. The application of this defense system demonstrated its effectiveness during the Israeli–Palestinian conflicts.

Michael O'Hanlon conducted comprehensive research on the protection of military bases and global security strategies, as well as on the logistical protection and defense of military units, and provided analyses of U.S. military security policy and base protection [5].

Paul K. Davis developed analytical approaches and models for the protection of U.S. military units and conducted research on modeling military strategy and defense systems, including analyses related to "Force Protection." He proposed a number of recommendations on mathematical modeling and strategic planning for the protection of military facilities [6]. The United States occupies a leading position in the application of advanced technologies and cybersecurity policies in the protection and defense of military units, military facilities, and state infrastructure.

At present, the United States uses a multi-layered security model that integrates specialized units from major service branches. This structure includes the U.S. Army Military Police, U.S. Air Force Security Forces, Navy Masters-at-Arms, and Marine Corps security personnel. Army Military Police and garrison units—amounting to nearly 100,000 personnel—provide physical protection of facilities through advanced surveillance, access control, and rapid response teams. In the U.S. Air Force, approximately 45,000 security forces protect air bases and aircraft using state-of-the-art electronic surveillance, perimeter intrusion detection, and network-centered rapid response capabilities [7].

The advantages of integrated security paradigms are reflected in the U.S. security model, which is distinguished by the following key principles: specialization and integration among different branches of the armed forces, enabling improved rapid response mechanisms through cooperation between military police, air, and naval forces; integration of physical and cybersecurity, where electronic surveillance systems, automated threat detection, and cyber defense measures are implemented simultaneously; and digital command and artificial intelligence, with AI and automated monitoring systems used for real-time situation analysis and strategic decision-making.

Japan's defense strategy is implemented through the Japan Self-Defense Forces (JSDF). Military facilities in Japan are protected through three main components: the Japan Ground Self-Defense Force (JGSDF), which protects strategic bases using biometric authentication and advanced surveillance systems; the Japan Air Self-Defense Force (JASDF), which ensures air security through the Mitsubishi Electric J/FPS-5 radar system and the Patriot PAC-3 missile defense system; and the Japan Maritime Self-Defense Force (JMSDF), equipped with the Aegis combat system and Type-12 coastal defense missiles.

In Germany, security is ensured under the command of the Feldjäger (military police): Siemens Siveillance systems are used for biometric access control and perimeter protection; Rohde & Schwarz ARDRONIS provides counter-drone surveillance and automated threat detection technologies; and Hensoldt SPEXER 360 offers 360-degree surveillance radar capabilities for early threat detection and neutralization. Germany applies a hybrid security model aligned with NATO strategies.

However, according to the geopolitical analyst V. A. Dergachev, although scientific and technological progress prevailed in the twentieth century, no solid scientific foundations have been created that would allow for logical and competent conclusions about the consequences of the global changes taking place on Earth and within individual countries [8]. Indeed, today there is a noticeable shortage of professional military specialists capable of possessing a broad and strategic worldview, global thinking, rapid decision-making in specific spaces and situations, and choosing the correct course of action—something clearly demonstrated by the Russia–Ukraine and Israel–Palestine cases.

In developed countries (Germany, France, the United Kingdom, Japan, China, and Korea), the integration of video surveillance systems and guarding activities serves as an important deterrent against various types of offenses. While surveillance cameras function as visible deterrents, security personnel enhance overall security through their physical presence.

The integration of these two security components has created a high-level security system, significantly reducing the likelihood of illegal activities.

In the United States, Germany, the United Kingdom, and France, the protection of critically important facilities is carried out by military police, guard units, and private security organizations. The protection of especially important and classified facilities is entrusted to special military units. Within the U.S. defense industrial base plan, a national infrastructure protection framework has been developed through coordinated efforts between public and private sector partners, ensuring risk management systems adapted to sector-specific characteristics and threat contexts. The Ministry of Defense has assigned special units of the Sector Risk Management Agency with responsibilities for guarding and protecting the defense industrial base sector. In the U.S. Department of Defense, the protection of military industrial bases, airfields, underwater and surface vessels, space rocket complexes, and strategically important state facilities is carried out in accordance with the risk and threat prevention plans of the Sector Risk Management Agency, demonstrating high effectiveness today.

For China, the launch of the “Belt and Road Initiative” became a decisive factor in establishing militarized organizations. At the same time, for a number of reasons, China found it impossible to openly use legal instruments or military force abroad. Outside China, approximately 3,200 employees of private Chinese security companies were officially operating, and there is no doubt that this number has since increased [9]. In addition to protecting facilities and individuals, private security companies engage in intelligence collection and analysis, development of comprehensive security plans, risk and threat assessment, logistical and informational support of security systems, incident investigations, and other functions traditionally associated with state special services.

Another factor contributing to the improvement of guarding activities is the increasing effectiveness of unmanned aerial vehicles (UAVs) in repelling air attacks and destroying key ground-based weapons during military conflicts. This also necessitates the development of measures for both the use of UAVs and protection against them. It is widely recognized that UAV-based attacks can be more effective than the level of protection applied to critical facilities.

According to some data, FPV (first-person view) drones account for about 40 percent of frontline losses in the Ukraine war. High speed, precision, small size, and quantity have made quadcopters the most dangerous threat for both sides. Due to their low cost, these drones have become an essential weapon in the infantry arsenal. Currently, each frontline soldier reportedly

ISSN: 2053-3578 I.F. 12.34

has three to four quadcopters. In Ukraine, drone operators control UAVs from fortified positions, ensuring soldier safety while monitoring unit movements. Mavic drones (factory models) have a maximum speed of about 60 km/h, whereas militarily modified FPV drones can reach speeds of up to 100 km/h. In addition, Ukrainians are developing their own models based on the Mavic platform. According to Reuters, the country produces up to four million UAVs annually, including kamikaze drones, bombers, reconnaissance drones, and long-range strike drones. This production is carried out by private enterprises and volunteer groups.

Electronic warfare systems can be either stationary or mobile. The former protects a specific frontline sector or military facility, while the latter can be carried by infantry soldiers or mounted on armored vehicles. However, this technology also has limitations: to suppress drone signals, the operating frequency must first be identified.

The fiber-optic cable drones used by the Russian army represent a modern trend in military affairs that has not bypassed Uzbekistan. Previously, the country met its needs in this field through external suppliers, but since 2022, unmanned aerial vehicles have begun to be produced domestically. Drones for various purposes are being supplied to the Armed Forces under the “Lochin” brand. They were publicly demonstrated for the first time at an exhibition of innovative defense technologies held in Tashkent this year.

The emergence of drones on the battlefield has led to radical changes in military affairs. This represents a revolutionary step comparable to the introduction of gunpowder, tanks, or aviation in warfare. However, it is still too early to claim that technology will fully replace frontline soldiers. In this regard, forces with high technological potential will gain an advantage. The emergence of artificial intelligence has ushered in a new era in security and defense, transforming traditional thinking and offering previously unimaginable opportunities.

In conclusion, the main part of the article describes several applications of artificial intelligence in the military domain, including cybersecurity, autonomous weapon systems, surveillance, and predictive analytics. In modern warfare, the ethical and legal implications of artificial intelligence, the challenges of autonomous decision-making, and the increased likelihood of unforeseen outcomes can be anticipated. The study examines how artificial intelligence affects security policy, how different states are adapting their defense strategies to leverage AI advantages, and how they are addressing issues such as accountability, transparency, and the risks of an AI arms race. It also analyzes how AI integration may

influence the balance of global power and how access to AI capabilities by various actors could reshape international relations and the geopolitical environment.

Based on the above, organizing facility protection measures in line with contemporary developments, training military units involved in these tasks, and equipping facilities with modern security technologies should be regarded as urgent priorities today. From this perspective, ongoing reforms in the organization of guard services can be seen as contributing to the enhancement of the country's socio-economic and defense potential.

REFERENCES

1. Global Firepower. (n.d.). Global Firepower – World military strength rankings. https://www.globalfirepower.com.

2. Kun.uz. Ukraina dunyodagi eng yirik qurol importchisiga aylandi. 2025, February 10. https://kun.uz/kr/news/2025/02/10/ukraina-dunyodagi-eng-yirik-qurol-importchisiga-aylandi

3. Martin C. Libicki. RAND Corporation - Cyberdeterrence and Cyberwar. U.S. Must Focus on Protecting Critical Computer Networks from Cyber Attack. 2009. https://www.rand.org/pubs/monographs/MG877.html

4. David E. Johnson. Hard Fighting: Israel in Lebanon and Gaza. Monograph, RAND ARROYO CENTER SANTA MONICA CA, 2011. P.266. https://apps.dtic.mil/sti/citations/ADA555762

5. Michael O'Hanlon. The Science of War: Defense Budgeting, Military Technology, Logistics, and Combat Outcomes 2009. Princeton University Press. Princeton - The Science of War. https://press.princeton.edu/books/paperback/ 9780691157993/the-science-of-war?srsltid.

6. Paul K. Davis. Analysis of Strategy and Strategies of Analysis. RAND Corporation. Published Sep 4, 2008. https://www.rand.org/pubs/authors/g/gompert david_c.monographs/MG718.html.

The Defense Post. UK defense spending report. 2024, February 12. https://thedefensepost.com/2024/02/12/uk-defense-spending-report/

7. Cybersecurity and Infrastructure Security Agency. (n.d.). Government facilities sector. U.S. Department of Homeland Security. https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/government-facilities-sector

8. Дергачев. В.А. Геосиёсат.М., ЮНИТИ-ДАНА, 2004,с.3.

9. Topwar.ru. Как и где работают китайские ЧВК. 2021. https://topwar.ru/95478-kak-i-gde-rabotayut-kitayskie-chvk.html