BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

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

Tenchi warfare – modern military operations based on the "tenchijin" philosophy

Captain (Nv) (r) Sorin TOPOR, Ph.D.*

*Cyber security expert, National Institute for Research and Development in Informatics – ICI Bucharest/Associate member of the Romanian Academy of Scientists
e-mail: sorin.topor@ici.ro

Abstract

In the context of the ongoing conflict in Ukraine, the protection of material and human resources is an essential condition for regional security. The paper examines a number of trends in technological development, lessons learned from this conflict, and opportunities for applying the Japanese tenchijin philosophy to modern military operations. We propose that under the name of "Tenchi warfare" we highlight the role of advanced military technologies in military operations, with an emphasis on the exploitation of obscure spaces and knowledge, to ensure strong decision-making support in order to synchronize the rhythm of the engaged forces with the rhythm of enemy evolution. Similar to how ninja fighters approach combat, we believe such a strategy could be useful in offensive reactions in various domains, as well as for enhancing national and regional security.

Keywords:
Ukraine conflict; advanced technologies; tenchijin philosophy; tenchi devices; tenchi warfare; national security; military operations.

Article info
Received: 11 November 2024; Revised: 29 November 2024; Accepted: 2 December 2024; Available online: 17 January 2025

Citation: Topor, S. 2024. "Tenchi warfare – modern military operations based on the "tenchijin" philosophy". *Bulletin of "Carol I" National Defence University*, 13(4): 206-220. https://doi.org/10.53477/2284-9378-24-59

The Ukraine conflict has put humanity in front of military operations that can no longer be included in the provisions of the traditional laws of war and other related international conventions. Even if in this space there are destructive strikes on infrastructure elements, by both actors involved, after more than two years there is no declaration of war. Moreover, based on the Internet, extensive propaganda, cyber-attacks, and deep-fake campaigns are carried out with the role of forming and stimulating some opinion trends, which support an ideology, a policy, or something else that will attract sponsors, which can be governments, military-political organizations, NGOs, associations, etc.

In this context, emerging and disruptive technologies hold the most important position, being implemented in weapon systems and other military equipment, but also in systems intended for monitoring and management of regional and international security. The lessons learned from Ukraine allow for the formulation of general observations that compete with the reality that in order for an actor to be able to maintain its dominant strategic position in a certain field, it will have to use advanced technology, which mainly allows it to effectively exploit information resources.

Based on the study conducted, we believe that the identification of obscure elements in various strategic fields, by exploiting information resources, in addition to knowing the adversary, understanding his intentions, hiding his own strategic and operational directions, etc., favors approaches that surprise the adversary, hitting his weak points, with limited resource consumption. By appealing to the Japanese "tenchijin" philosophy and using ML/AI algorithms the rhythm of the military operation can be harmonized with that of the adversary. Similar to ninja tactics, it is observed that a slower rhythm can sometimes lead to the creation of obscure spaces that favor the execution of an attack and surprise the opponent in positions or areas over which, at the respective moment, he cannot achieve effective governance, his attention being focused on other operational elements.

About the japanese "tenchijin" philisophy and some methods of application

The "tenchijin" philosophy was the basis of the training of ninja fighters in ancient Japan and China. The origin of the concept comes from Japanese philosophy, which was inspired by the Chinese archetypal definition and has in its composition the three elements of the structure of the universe: Heaven (or air/ sky meaning "ten"), Earth (or the ground/ the soil under feet meaning "chi") and Man (or human/ mankind meaning "jin"). It symbolizes the balance and unity between the various elements of the universe and can be associated with the concepts of "yin" and "yang", which reflect the duality and interdependence between the different aspects of existence. Coming from the earliest times, when people practiced agriculture and animal breeding, life was sustained by knowing the influences of the smooth rotation of

the four seasons. This rhythm influenced production, belief, and politics. The crisis solution which could lead to war, was strictly determined by when the conditions of the sky, the earth, and human activities were aligned.

Thus, it became a principle of government and military strategies, being formalized and described by the famous military strategist Sun Tzu, in his work, "The Art of War". The strategy of "fighting without fighting" described by Sun Tzu is based on ways of using techniques to avoid direct contact where the opponent is strong and aware, by actions designed to disorient him, desensitize him and, most importantly, the attack should be carried out in ways that the enemy does not expect (Tzu 2026, ch. 8). For this, the three elements are applied on three levels (long, medium and close), from the 8 cardinal directions. Heaven represents the higher position that establishes order. Observance of heavenly orders ensures life (adaptation to the heavenly way means growth). Earth represents the lower position characterized by strength and power. If there is strong will there will be peace. Man holds the middle position. Therefore, all human activities must be performed according to correct rules and in harmony.

The practice of martial arts is based on the wisdom and cognitive power of the practitioner. The training of a ninja fighter was not limited to the practice of fighting techniques but also involved the development of knowledge in astrology and the cosmos, geography, and meteorology. All this knowledge allowed him to understand his position in space in relation to the opponent and how to place himself in relation to him. His disguise methods were an extension of this knowledge. A ninja was prepared to play various roles, having an appropriate outfit, using a language particular to the role performed, as well as a specific behavior that would allow him to complete the mission. Apart from understanding the conditions of space, it was especially important to frame his action in time. The ninja fighter could sense when the opponent's focus changed. Depending on this, he would adopt a slow rhythm, to induce confusion and not be synchronized with the opponent's rhythm.

To complete the counter-attack, an essential condition is to get back in the opponent's rhythm synchronization. His movement will be quick and successive, having the advantage of hitting from the not visible space by the opponent. It can be direct or indirect for added confusion. In addition, the ninja fighter can identify new vulnerabilities in the opponent's defense system, which inevitably arise due to his movement in the attack.
Thus, the ninja fighter meets an attack with various shirks and counterattacks. To become invisible, he understood when to use the smoke grenade and which direction to shirk when the opponent's sword struck. He understood that the arm holding the sword would cover the attacker's eyes, especially if he struck from up to down.

The Japanese dictionary suggests, metaphorically, that this technique represents „going in search of freedom" (Goo 2024). Developing this art of fighting, the

whole Sun Tzu's thesis shows how an opponent can be attracted into an illusion based on deception. The basic condition is that the one who exploits this science has the advantage of knowing and understanding the adversary's vulnerabilities. In the required situation, the opponent's sensory elements are directly hit (for a ninja, damage to the opponent's eyes creates the opportunity to reach unattended spaces).

Creating invisible spaces for the opponent is a strategy that increases the chance and safety of one's own action. If the opponent's attention is focused on the suggested place, his perception of reality is distorted. In an extremely simple way, we appreciate that the strategy of conflict based on the tenchijin philosophy is the art of using obscure spaces and adapting the rhythm so that an action is effective in accordance with the planned objective.

Generalizing, we note that martial arts practitioners do not openly manifest their attack intentions. They have the ability to exploit atypical environments and spaces, eccentric to their relational system. Thus, allowing an opponent to be focused on an illusion will place them in a disadvantageous zone for the opponent. Starting from these principles, applications have been developed in numerous fields, such as medicine, economy, politics, urban planning, security, etc. Even in the field of entertainment, all „magicians", in their performances, use obscure spaces and shift the audience's attention to another movement, achieving tricks in which objects disappear or appear.

Currently, many economic entities in Japan are exploiting these techniques based on the use of spatial information, in order to estimate obscure spaces and land evaluation. These applications are said to be useful in agriculture, fishing, real estate, energy, logistics, tourism (Jaxa 2019), etc. For example, based on the GIS service and using machine learning algorithms (ML/AI), the risks of leaking water pipes can be managed (Tokyo SME 2023). Yasutoshi Hyakusoku, co-founder of the Start-up „Tenchijin" and head of the R&D office/ JAXA (Japan Aerospace Exploration Agency) states that if it has been shown that a large part of economic problems can be solved by technology, there are also social challenges whose solution, even if it is not easy, could be solved in this way, both globally and locally. Hyakusoku believes that „sensors or telecommunications equipment from space that observes the Earth should be part of the planet's infrastructure" (Spotlight 2023).

Within business ecosystems, corporations are increasingly facing cyber-attacks, especially in their relationships with third-party partners and suppliers. Innovative and disruptive solutions are used for cyber risk management in order to provide cyber security services. Endeavor's Scale Up Outliers program (Tenchi 2024) aims to reduce information asymmetry in information security and compliance risks in corporate ecosystems in a cooperative and scalable manner to return on invested capital. Even though these developments have advanced many fields, leading end-to-end cybersecurity services focused on protection strategies, resilience and a range of

industry-specific services have also attracted the attention of some armies, especially in the cloud environment and the organization's ecosystem governance domains.

Being an extremely important field, there is no public information about these services, in which case, our analysis will be limited to tenchijin philosophy approach principles and the effective use of emerging and disruptive technologies. These, having a huge potential to contribute to public security, can always become targets in various attacks, in the context of the existence of a variety of military interventions in the world, but also in other types of international relations.

Advances technologies in the russo-ukrainian war

In the history of humanity, especially in periods of changes in the balance of power of the international order, many conflicts are present. Russia's aggression against Ukraine is a violation of all the rules, and the danger of this pattern is determined by the possibility of a similar situation occurring anywhere in the world. Thus, the risks to regional and global security, on the background of increasing pressures to change the status quo by military force, are complex and increasingly hybrid and can be amplified by the proximity of a country that has a strong army, nuclear weapons, and a real industry of war.

Looking at the current geopolitical context, it is observed that the "frozen wars" and "gray zone" situations of some territories, the expansion of other "gray zones" of postmodern war, combined with transboundary cyber-attacks on critical infrastructures, information controlled, propaganda and deep-fake etc., dilutes the power of the recognized norms between the state of war and those of peace. Domains of national security, previously considered non-military, have been expanded into economic and technological directions. These approaches result in making it excessively difficult to draw the line between military and non-military conflict.

The irony regarding the current state of international security is that all the unprecedented measures and sanctions taken against Russia, even if they aimed to oblige to stop fighting, risk increasing material destruction, increasing the number of victims, and the duration of the conflict. In addition, the confrontations between regimes (Democratic vs. Autocratic), the blending of military and political components, the struggle to obtain dominance in any domains, etc., created uncertainty in establishing the responsibility of the aggressor, in the event of the war starting. Cross-border incidents, missile and drone strikes, sabotage and incursions, destruction and loss of human life, etc., especially following Ukraine's incursion into Russian territory, have heightened regional tensions and created the conditions for a long-term war, with new, associated risks.
These unprecedented military operations could not be possible without the use of advanced technologies, which revolutionized the entire military ecosystem, and influenced the strategies and battles.

We present the main advanced technologies used in the conflict in Ukraine:

A. Drones. Before the beginning of the Russian special operation against Ukraine, even the biggest supporters of the promotion of unmanned aerial systems (UVS) could not have estimated the extent and diversity of the fields of exploitation of drones. After only two and a half years of war, the use of drones is essential for precision strikes and tactical reconnaissance/observation. Drones are capable of operating in information networks based on satellite systems, terrestrial communications networks, and human agents (HUMINT). The information on these devices allowed the rapid assessment of the tactical and operational situation. Thus, against Russian drones, the Ukrainians use miniaturized "tenchi" devices and portable electronic warfare systems. Russia's response was to launch attacks by Lancet kamikaze drones that recognize the target recognition signals, generated by Orlan-10 and SuperCam drones, in the visual and infrared spectrum (Battersby 2024). With this equipment, Russia sought to match the performance of Ukrainian strikes with HIMARS systems (provided by the US) (Farrell 2023), against artillery, tanks, and other high-value targets.

B. Electronic warfare (EW). Due to the particularities determined by the mobility and the increased requirements of information exchange, ensuring the security of the resource of electromagnetic frequencies, attacking the similar resource of the adversary is a main objective of contemporary military operations. Through electromagnetic waves, the coordination and synchronization of actions are achieved, the public's right to information and social communication links are ensured, and the security of critical infrastructures and the protection of the civilian population in the geographical areas related to the conflict are maintained. In this context, electronic warfare equipment is essential for disrupting the adversary's communications, hindering coordination, and disrupting the efficiency of his actions, in an environment where the limits of the electromagnetic frequency spectrum cannot be expanded. Thus, electronic warfare has moved from the stage of active networking to that of active confrontation, constituting a condition for winning and maintaining the initiative.

The Russians, unlike NATO countries, have operationalized electronic warfare at all hierarchical levels (strategic, operational, and tactical) and in all components of its army (land, sea, air, and space). EW forms the basis of information warfare doctrine (Chiriac and Withingon 2024). In fact, David T. Pyne, a researcher at the EMP Task Force and former director of the US Department of Defense, estimates that Russia has "the most capable electronic warfare system in the world" (Giangiulio 2023), being impressed by the speed of adaptation at the performances of latest US and NATO weapons systems.
Russian electronic warfare equipment has been able to render the Excalibur, GLSDB, and HIMARS technologies ineffective by jamming satellite signals (Skove 2024). They disrupted the Starlink Internet capabilities, provided by the Pentagon, complicating the coordination of forces and the launching of Ukrainian drone

strikes (Mozur and Satariano 2024). In this war, Ukraine would not have lasted so long without the support of technology companies from the US, Europe, and Asia who provided high electronic and cyber technology that allowed them to use the weapons systems (Topor 2024).

Moreover, the Ukrainian military forces in the incursion at Kursk (August 2024) benefited from effective EW support, which supported the creation of obscure spaces in the Russian defense. Success would not have been possible without information, timing, and decision support. This military force involved hundreds of Ukrainian troops, infantry units, mechanized units, and drone support. The operational surprise was evident, and the response of Russian forces was far too slow to stop the offensive and push the Ukrainians across the border. Still, electronic warfare should not be confused with cyber warfare and other hacking techniques (NATO 2023) of electronic devices.

C. Cyberwarfare: Cyberwarfare, and especially the cyber defense component, has become a critical component of Ukraine's national security strategy. Cyberspace is recognized as the fifth domain of war, along with land, air, sea, and space (Avanesova, Serhiienko and Lyubushin 2022, 25-40). Mainly, the cyber dimension of warfare is a dominant component in the battle for online information, from campaigns to winning hearts and minds (Willett 2022). In this conflict, cyber warfare can be classified into three levels of approach, namely: destructive cyber-attacks, network penetration for espionage activities, and last but not least, psychological influence operations of the international audience through cyber sociology products. Against it, Ukraine could not have coped with the situation without Western and NATO support.

Through the Internet, the emotions of anyone interested in this event were stimulated by messages guided around key terms such as war, victory, death, destruction, fear, migration, etc. Thus, a semantic space was created for the application of AI/ML search engine algorithms, as well as a series of meta-tags within social networks, as response strategies for the radicalization of the international audience. Thus, alliances of states, coalitions of companies from the public or private sectors, and NGOs were formed, which supported one of the two actors involved. Official and unofficial narratives varied significantly, depending on the source, and accompanied direct contact between the armed forces. Usually, the Russian component characterizes the fighting as a form of defense against terrorism and other highly aggressive provocation movements of Ukraine, as a direct action on national sovereignty, and as a measure to increase security against the nazification of the Russian population by the Ukrainian regime. On the other hand, Ukraine praises the bravery of its armed forces, makes accusations of war crimes, and calls for Western defense support.

Through cyber-attacks, presidential elections were manipulated, energy distribution companies, financial institutions, postal services, news publications, transport and commercial services were hit, government web pages and even telecommunications

services that were provided through the Starlink satellites system were affected. The symbolic value of Ukraine's cyber defense far exceeded the operational value of the military maneuvers, demonstrating the resolve and sustainment of Ukrainian combat capabilities (Youvan 2024).

D. Missile systems and precision artillery. In the field of weapons, advanced technologies have been implemented in strike systems to increase the accuracy of strikes (especially on infrastructures of strategic value), reduce collateral damage, as well as to improve operational efficiency. At the tactical level, the missile and artillery systems used by both actors led to the so-called artillery genocide (70% of Ukrainian casualties are caused by Russian ground artillery), with Ukrainian forces dealing only with self-propelled artillery, received as aid (Buță and Manoliu 2023, 168-175). At the strategic level, Russia's development and use of hypersonic missiles have prompted a review of European and NATO defense and risk assessment strategies, and it is quite possible that Russia might continue to develop appropriate, high-speed, nuclear-extended capabilities (Wright 2022). Although these challenges can be mitigated through international technical and political mechanisms, potential manufacturers can continue to invest in scientific research and technological testing leading to new systems whose performance exceeds current ones.
For example, Ukraine uses Switchblade missiles (v. 300 and 600), a tactical missile-drone-AI combination with autonomous capabilities, ground-launched and autonomous target-locating and systems-priority strike capabilities of anti-aircraft, tank, and other Russian defense systems (Cook 2024).

E. Artificial intelligence (AI). AI algorithms have improved data analysis, mission planning, and resource optimization. Thus, the speed and accuracy of decision-making activities in numerous military and civilian fields have been increased. Military decision-making structures can use AI in operational and tactical fields to predict conflict zones, optimize evacuation routes, or prioritize the treatment of the wounded (Kolesnikov and Kryzhevsky 2023). At a strategic level, AI can be used to support foreign policy decisions and diplomacy (Sirenko 2024, 122-128), manage emergencies, rebuild infrastructures, and even counter disinformation (Kertysova 2018, 55-81). It should be noted that the war in Ukraine has caused a very rapid development of autonomous systems based on AI, the involvement of which has changed the dynamics of combat maneuvers. In addition to drones, EW, intelligence and cyber warfare systems use AI to collect data, spread disinformation (including image and video manipulation), intercept unencrypted communications, geo-locate and analyze open-source data to identify soldiers, weapons, systems, units, and their maneuvers (Marija and Vanja 2023, 59-76). This does not mean that the role of conventional weapons is ignored. The essence of the use of AI in armed conflicts is reflected in the economy of human resources and the reduction of casualties.

F. Secure communications. Advanced communication technologies have improved communication methods to coordinate maneuvers between units and transmit

information quickly and securely. Obviously, digitized technological solutions have provided the opportunity to create new governance systems that have allowed the optimal use of resources, the modernization of policies and specific services, as well as the effective interaction of all structural units, military and civil, at all hierarchical levels. In this regard, data and information protection has become not only a technical but also a legislative issue for the Ukrainian government and beyond. From a technical point of view, the use of Starlink satellites has brought enormous benefits to keeping many communications services intact, especially for forces engaged in warfare. In addition, a number of administrative structures have been created and developed to ensure the security of public services, in electronic forms, such as the iGov.org web portal, the Kiev Tsyfovii application (for using various community services via smartphone), other applications that ensure several functionalities related to the hostilities on the territory of Ukraine (shelter map, map of an ongoing business, voluntary help of the army, voluntary assistance, links to official sources etc.) (Bojor, Petrache and Cristescu 2024, 185-194), strengthening social resilience.

G. Air defense: The war in Ukraine, in addition to drones, has also become a testing theatre for new air defense technologies. These were essential for protecting ground forces from Russian air strikes and missile attacks. In fact, the aspects regarding the modernization of Ukrainian air defense systems have been the subject of many publications, following the whole range of systems, with long, medium, short, and close range of military equipment complexes (Spirin, Pogorilyi and Shynkarenko 2023, 75-81). The new systems included new optoelectronic technologies, for accurately determining the coordinates of the target, for faster detection and reducing the reaction time to changes in the operational situation, electronic attack protection components, mobility and obstacle-overcoming capabilities, etc. Due to the time constraints associated with the deployment and testing of new systems in combat, a number of limitations have also been identified, which are mainly determined by ensuring compatibility with other weapons, communications systems, and drones. On the background of the support of Ukraine by European countries and NATO with modern equipment, Russia could not ensure its air superiority, being forced to change its tactics of using air power, focusing its effort on missile and drone strikes. Unfortunately, the situation of the Russian Federation's lack of control of airstrikes, with cruise missiles and drones, continues to cause many casualties among Ukrainian civilians (Титаренко and Власенко 2024).

H. Education and training technologies: Advanced simulation technologies have enabled effective training, adequate training of soldiers to deal with various combat scenarios, and improvement of their reactions under conditions of stress and uncertainty. Among the many technological innovations intended for military training, we mention virtual multimedia simulators, educational games, automatic knowledge assessment systems, distance learning equipment, etc. The use of these educational tools, in addition to improving the efficiency of training and motivation, also allowed the reduction of time and related costs. This improves applied military

education, the quality of learning materials, and assessment models. This approach aligns with the trend of integrating advanced information technologies into military education, becoming a crucial tool for modernizing military education and training. Effective solutions are provided for the use of sensors, weapons, and other combat systems to meet the evolving needs of the armed forces in the context of ongoing warfare. In addition, these solutions are also useful in raising the morale of Ukrainian troops, supporting the motivation to respond to hybrid threats, training military specialists, and developing skills in the use of weapons, in accordance with NATO standards (Kozubtsov et al. 2023).

Generally, we appreciate that the military operations carried out in this conflict demonstrate the importance of collaboration and coordination of the maneuvers of the components of the armed forces structures, in order to obtain the tactical and operational advantage. This involves synchronization and efficient exchange of information and resources. We estimate that in line with the development of advanced technologies towards digitization and miniaturization, weapon systems and military equipment will be increasingly numerous, more precise, more efficient, and integrated, as the electromagnetic environment and cyberspace will become indispensable for any type of warfare.

Analysis and discussion of "tenchi" military operations

Current advanced technologies favor the production of a multitude of relevant information, analysis, and predictions, which, with appropriate learning and training in order to develop knowledge, can represent the basis of effective management in a diversity of fields. The category of tenchi electronic devices includes smartphones, smart health monitoring devices, smart watches, and other types of portable electronic devices that use big databases and communication networks. All of them contain advanced communication technologies, such as Bluetooth or Wi-Fi, sensors for measuring various parameters (from health to environment), intuitive interfaces, algorithms, and other applications that support human activity. Tenchi devices are also included in industrial machines that, depending on the environment of use, can perform various activities from product packaging to food processing (Tenchi Sangyo Co. 2021).

Conceptually, there is no category of activities that can be identified with this name. „Tenchi warfare" is a screenplay of the animated film „War on Geminar", a spin-off of the Japanese series Tenchi Muyo! We consider that the hypotheses addressed in this film can become reality in the conditions in which disruptive and emerging technologies are increasingly present in everyday life. The video game based on this film puts participants in combat scenarios between samurai and ninja characters with special abilities to navigate complex levels, avoid enemies, eliminate targets, steal information, and rescue hostages, all without being detected. A variety of

weapons, combinations of strategic actions, and stealth tactics lead to the resolve of missions to uncover political conspiracies and avenge betrayals, obviously in the Japanese feudal atmosphere. The game puts players in front of moral choices that can affect the story and relationships with various characters. The multiplayer mode allows players to compete against each other using stealth, camouflage, and disinformation skills.
A game apparently similar to those from the „capture the flag" or „assassination" class, it is quite addictive in digital media. Yet, similarly to other strategic war games, they can form wrong perceptions of the ethical and moral norms of war for a young person with no military training

For military science analysts and researchers, it can be a useful tool to understand some aspects of techijin philosophy. Practicing stealth techniques can develop skills for identifying obscure spaces and a mission rhythm, which can then be practiced in real life in a complex environment with asymmetric and hybrid risks and threats.
It is well known that the notion of cyber warfare was developed around the concept of cyberspace. The paternity goes to the novelist William Gibson who, in his book Neuromancer (1984), established through cyberspace a virtual space, beyond the physical world, accessible through computer networks, having a strong impact on the vision of what the current Internet represents. With the introduction of the Internet into military operations, cyberspace has become a core concept that sets the environment for information warfare, with individuals who can attack and/or determine a high level of security for computers and computer networks (Van Haaster 2019).

Similarly, we define the concept of „tenchi warfare" as those strategies and methods of warfare based on advanced technologies, emerging and disruptive technologies, on the enemy's critical infrastructures, manipulating information, anticipating developments and projecting power, as well as ensuring security against risks and hybrid threats. From an ethical and moral point of view, a big problem is the use of manipulation to destroy a social system, organized around a certain ideology. We pointed out that terrorism and long-range strikes are meant to achieve destruction and loss of human life in warfare that cannot be framed in international law under the concept of war.

Currently, the opportunity to exploit advanced technologies in warfare largely ensures victory. The challenges regarding the protection of critical infrastructures and the civilian population captive to the conflict space are derived not from the use of emerging and disruptive technologies, but from the purpose for which it is used. In this context, we believe that military operations based on the art of tenchijin can be planned and executed, which we include in the concept of „tenchi warfare".
For example, even if the falsity of the Russian motivation regarding the legalization of the war against Ukraine is recognized (Russia invoked maintaining peace in the

Donetsk and Lugansk regions, as well as stopping the genocidal crimes committed in the eastern Donbas region) and determined an international mechanism to establish the perpetrators' crimes during the war, Russia used military force and occupied several critical and strategic Ukrainian locations (Khater 2022). Ukraine's reaction, under intense information warfare and under strikes that include advanced technologies, can be considered a tenchi operation, based on strategies that established a high level of collaboration and effective coordination of forces, adjusting the rhythm of defense operations to the rhythm of the Russian offensive, the execution of offensive counterattacks in areas and with methods that allowed him to surprise the opponent.

No one expected that on August 6, 2024, two and a half years after the start of the war, Ukrainian troops would make a successful incursion into Russian territory, reaching Kursk. Remarkable are the scale and speed of this military operation, the knowledge of the reality of the reaction power of the Russian forces in the defense breach area, as well as the way of preparing the entire military operation, under the umbrella of unprecedented security measures. Thus, Ukraine established a buffer zone to prevent the bombing of its territory in the Kursk region, an additional pressure on Russia (which was obliged to transfer troops from another contact zone to stop the offensive) and an imagological gain, essential in restoring the morale of the troops and civilian population.

Moreover, this strategy allowed the rapid acquisition and maintenance of tactical and operational advantages in numerous areas, among which we enumerate:

1. Exploitation of Russian defensive weaknesses, improved penetration tactics, and combined use of advanced technology, GIS intelligence, drones, sabotage actions, precision strikes, and maneuver strategies;
2. International support with modern equipment and systems, adapting and reforming tactics according to combat capabilities;
3. Improved mobility and attack capabilities focused on the enemy's weak points;
4. Demonstrating the effective use of information capabilities to demoralize Russian troops and mobilizing public opinion to increase national solidarity;
5. Expanding defense and tactical adaptation capabilities depending on the type of battle (urban warfare, open ground warfare, electronic warfare, etc.);
6. The recapturing of territories that allowed a controlled withdrawal from other areas, followed by quick and effective counterattacks.

We appreciate that this incursion can be similar to the counterattack of a ninja who has understood how to use, in his favor, obscure spaces and domains, in the background of an adapted rhythm of strategic defense, followed by a quick offensive reaction, until the moment when the planned objectives are achieved.

Conclusions

In the context of digital transformation and the development of emerging and disruptive technologies, the growing trends of the defense and security equipment market, the implementation of technological advances in increasingly complex systems, and the ability to stimulate scientific research and the production of new equipment, with significant investments in various fields, etc., the proposed concept of "tenchi warfare" can characterize this historical moment in the evolution of military art. Currently, even though many different factors depend on the regional geopolitical and military context, every country is aiming to strengthen its defense capabilities and improve its military training.

The concept presented is a hypothesis of scientific research, resulting from the descriptive analysis of the Japanese philosophical concept, applied to advanced technologies for the military field, based on which, through a series of modeling, simulations, and tests, it can be established how useful it might be in this regard and what the conditions are for its implementation in military operations. Such an approach can be useful both in the phase of establishing the combat platforms design, in the stability of the level of armament, etc., and the stability of strategies for reorganization of combat units.

Moreover, we consider that strategic planning, developed through such an approach, can outline effective directions for the development of the future military industry for strengthening the security of critical infrastructures, with the main requirement being the protection of human resources, in the context of hybrid attacks, supported by an intense information warfare. We estimate that other directions related to the strengthening of national security with a strong positive impact on the national economy can be developed.
Through the multitude of domains addressed, we emphasize that this study is a commitment that our research will continue and the results obtained will be published in future works.

References

Avanesova, N.E., Y.I. Serhiienko, and R.A. Lyubushin. 2022. "Strengthening the State Cyber Defence and Creating of Cyber Troops: State, Problems and Organizational – Economic Measureas for Ukraine." *Economic Innovations* 24 (1): 82. https://doi.org/10.31520/ei.2022.24.1(82).25-40.

Battersby, Blair. 2024. *Russia Struggling to Integrate Its Most Effective Unmanned System, TRADOC G2.* https://oe.tradoc.army.mil/2024/04/18/russia-struggling-to-integrate-its-most-effective-unmanned-system/.

Bojor, Laviniu, Tudorică Petrache, and Cristian Cristescu. 2024. "Emerging Technologies in Conflict: The Impact of Starlink in the Russia-Ukraine War." *Land Forces Academy Review* 29 (2): 185-194. https://doi.org/10.2478/raft-2024-0020.

Buță, Viorel, and Răzvan Manoliu. 2023. "Noi tendințe în întrebuințarea diferitelor arme în războiul Ruso-Ucrainean." *Conferința științifică internațională „Gândirea Militară Românească", Teorie și Artă Militară.* doi:doi.org/10.55535/gmr.2023.4.09.

Chiriac, Olga R., and Thomas Withingon. 2024. *Russian Electronic Warfare: From History to Modern Battlefield, Irregular Warfare Initiative.* https://irregularwarfare.org/articles/russian-electronic-warfare-from-history-to-modern-battlefield/.

Cook, Ellie. 2024. "US-Made `Tank-Killer` Switchblade Destroys Russian SAM System in Rare Video." *Newsweek.* https://www.newsweek.com/ukraine-switchblade-drone-russia-tor-air-defense-system-video-1976448.

Farrell, Francis. 2023. *How Russia's homegrown Lancet drone became so feared in Ukraine, The Kyiv Independent.* https://kyivindependent.com/how-russias-homegrown-lancet-drone-became-so-feared-in-ukraine.

Giangiulio, Graziella. 2023. "#UKRAINERUSSIAWAR. For Kiev it is the last chance but Moscow last the numbers to win on paper." *News AGC Communication.* https://www.agcnews.eu/ukrainerussiawar-for-kiev-it-is-the-last-chance-but-moscow-has-the-numbers-to-win-on-paper/.

Goo. 2024. *„Tenchi", [traducere din japoneză].* https://dictionary.goo.ne.jp/srch/jn/%E3%83%86%E3%83%B3%E3%83%81/m0u/.

Jaxa. 2019. "Introduction of JAXA ventures." *Tenchijin, Inc.* https://aerospacebiz.jaxa.jp/en/venture/tenchijin/.

Kertysova, Katarina. 2018. "Artificial Intelligence and Disinformation: How AI Changes the Way Disinformation is Produced, Disseminated, and Can Be Countered." *Security and Human Right* (No.29): 55-81. https://doi.org/10.1163/18750230-02901005.

Khater, Maya. 2022. "The Legality of Russian Military Operations Against Ukraine from the Perspective of International Law." *Access to Justice in Eastern Europe Journal.* doi:10.33327/AJEE-18-5.3-a000315.

Kolesnikov, E.B., and V.V. Kryzhevsky. 2023. "The use of Artificial Intelligence at the Stages of Evacuation, Diagnosis and Treatment of Wounded Soldiers in the War in Ukraine." *Kharkiv Surgical School* (no. 4-5 (September)): 80-83. https://doi.org/10.37699/2308-7005.4-5.2023.11.

Kozubtsov, Igor, Ihor Danyliuk, Andrii Krasnobokyi, and Svitlana Voronaia. 2023. "Prospects for the use of Virtual Reality Technologies in the training of military specialists (Tactical level of Military Education) according to the compatible NATO Standards." *Bulletin of Science and Education* 11 (17). https://doi.org/10.52058/2786-6165-2023-11(17)-770-784.

Marija, Doric, and Glisin Vanja. 2023. "The use of artificial intelligence in the Russo-Ukarinian war." *Politika nacionale bezbednosti* 25 (2): 59-76. https://doi.org/10.5937/pnb25-47369.

Mozur, Paul, and Adam Satariano. 2024. "Russia, in New Push, Increasingly Disrupts Ukraine's Starlink Service." *The New York Times.* https://www.nytimes.com/2024/05/24/technology/ukraine-russia-starlink.html.

NATO. 2023. *Electromagnetic warfare.* https://www.nato.int/cps/en/natohq/topics_80906.htm.

Sirenko, A.S. 2024. "The Role of Artificial Intelligence in Making Foreign Policy Decision in the Ukrainian- Russian War." *European Socio-Legal & Humanitarian Studies* (No.1): 122-128. https://doi.org/10.61345/2734-8873.2024.1.13.

Skove, Sam. 2024. *Another US precision-guided weapon falls prey to Russian electronic warfare, US says, Defence One.* https://www.defenseone.com/threats/2024/04/another-us-precision-guided-weapon-falls-prey-russian-electronic-warfare-us-says/396141/.

Spirin, Denis, Olecsandr Pogorilyi, and Olga Shynkarenko. 2023. "Justification of modernization paths for short-range air defense missile systems of land forces." *Scientific works
 Of State Scientific Research Institute of Armament and Military Equipment Testing and Certification* 16 (2): 75-81. https://doi.org/10.37701/dndivsovt.16.2023.11.

Spotlight, Japan. 2023. "The usages of Data from Space." *Special Interview.* https://www.jef.or.jp/journal/pdf/249th_Special_Interview.pdf.

Tenchi Sangyo Co., LTD. 2021. *Tenchi Sanhyo Packaging Machines.* https://www.tenchi.jp/en/aboutus/.

Tenchi. 2024. "Tenchi Security raises a $7 million Series A from Bradesco, L4 Venture Builder, and Accenture." *News.* https://www.tenchisecurity.com/en/insights-news/tenchi-security-raises-a-7-million-million-series-a-from-bradesco-l4-venture-builder-and-accenture.

Tokyo SME. 2023. *Leakage Risk Assessment & Management Software: Tenchijin CMPASS KnoWaterleak.* https://tokyo-smes.com/en/productservice/management-software/.

Topor, Sorin. 2024. "The importance of military sciences to ensure national survival in future conflicts ." *Journal: Annals – Series on Military Sciences* (No. 1). https://www.ceeol.com/search/article-detail?id=1248442 .

Tzu, Sun. 2026. *Arta războiului* . București: Editura Art.

Van Haaster, Jelle. 2019. "On Cyber: The utility of military cyber operations during conflict." *[Thesis, fully internal, Universiteit van Amsterdam], UvA-DARE (Digital Academic Repository).* p. 90. https://pure.uva.nl/ws/files/37093787/Thesis.pdf.

Willett, Marcus. 2022. "The Cyber Dimension of the Russia-Ukraine War." *Survival: Global Politics and Strategy* 64 (5): 7-26. doi:10.1080/00396338.2022.2126193.

Wright, Timoty. 2022. *Hypersonic Missile Proliferation: An Emerging European Problem?* EU Non-Proliferation and Disarmament Consortium, Non-Proliferation and Disarmament Papers, No.80. doi:doi.org/10.55163/qvhv3959.

Youvan, Douglas. 2024. *The Shadow War in Kursk: Assessing the Potential Role of CIA Covert Operations in the Ukrainian Incursion int Russian Territory.* doi:10.13140/RG.2.2.15318.46404.

Титаренко, Олександр, and Євген Власенко. 2024. "ПРОТИПОВІТРЯНА ОБОРОНА В РОСІЙСЬКО-УКРАЇНСЬКІЙ ВІЙНІ: УРОКИ ТА РЕКОМЕНДАЦІЇ" ("AIR DEFENSE IN THE RUSSIAN-UKRAINIAN WAR: LESSONS AND RECOMMENDATIONS")." *Повітряна міць України* 1 (6): 49–55. https://doi.org/10.33099/2786-7714-2024-1-6-49-55.