GELECEĞİN ASKERİ 2024
YENİ DÜNYA YENİ SAVAŞ YENİ SAVAŞÇI

FUTURE SOLDIER 2024
NEW WORLD NEW WAR NEW WARRIOR

TÜRKİYE CUMHURİYETİ MİLLİ SAVUNMA BAKANLIĞI

SSB
SAVUNMA SANAYİİ BAŞKANLIĞI

SASAD
SAVUNMA VE HAVACILIK SANAYİİ İMALATÇILAR DERNEĞİ

ORGANIZATION SUMMARY AND CONCLUSION REPORT

Platin Sponsor

Golden Sponsors

Silver Sponsor

Contributors

GELECEĞİN ASKERİ 2024
FUTURE SOLDIER 2024

ORGANIZATION SUMMARY AND CONCLUSION REPORT

SASAD
SAVUNMA VE HAVACILIK SANAYİİ İMALATÇILAR DERNEĞİ

Telephone: 0312 426 22 55

Fax: 0312 426 22 56

E-Mail: sasad@sasad.org.tr

Web Site: www.sasad.org.tr

Adress: Ankara Sanayi Odası Binası, Atatürk Bulvarı. No: 193, Kat: 6, Kavaklıdere, Ankara, Türkiye

Project Coordinator:

Türkünaz ÜNLÜ

turkunaz.unlu@sasad.org.tr

Editors:

Dr. Oğuz HAMŞİOĞLU

Türkünaz ÜNLÜ

Selahaddin KOYUNCU

Translate:

Ahmet Bera İLARSLAN

ISBN : 978-625-95822-0-7 (Hardback-Turkish)

ISBN Digital PDF: 978-625-95822-1-4 (Turkish)

ISBN Digital PDF : 978-625-95822-2-1 (English)

Project, Content and Event Agency:

AJANSBK

AjansBK Medya ve İletişim Teknolojileri Ltd. Şti.

Kavaklıdere Mah. Büklüm Cad. No: 22/6 Çankaya – ANKARA

0312 417 03 30 & 0534 321 46 55

Printing:

Tek Ses Ofset Matbaacılık Yayıncılık Organizasyon Hayvancılık Otomotiv Sanayi ve Ticaret Limited Şirketi

Kazımkarabekir Caddesi Kültür İş Hanı No: 7/60 Altındağ Ankara

Certificate No: 44186

This assessment, which covers these findings and recommendations, is based on the outputs of the Future Soldier 2024 event organized by the Ministry of National Defence (MoND), the Secreteriat of defence Industries (SSB) and the defence and Aerospace Industry Manufacturers Association (SASAD).

The organization was held on 26-27th November 2024 at the Ankara Space and Aviation Specialized Organized Industrial Zone (HAB) Conference Hall with the main theme of "New World, New War and New Warrior".

Experts from Turkiye and different countries of the world came together in the Future Soldier'24 organization had organized in a panel format and presented their recommendations on the military concept and technologies of the future in 10 different sessions. On the first day, the developments in future military technologies were discussed from an international perspective and on the second day from a national perspective.

The transcripts of the panelists' speeches have been transcribed from their presentations. The evaluations in this report are those of the speakers and reflect the views and recommendations of the institutions and their representatives.

SASAD Secretary General 2025

10	29	700	17
SESSION MAIN THEME MODERAT	SPEAKER	INVITED PARTICIPANT	SESSION DURATION

26-27th November 2024

Ankara Space and Aviation Specialized Organized Industrial Zone

Defence Technologies

covering military sciences as well, in the field of SCIENCE, TECHNOLOGY, ENGINEERING, and MATHEMATICS (STEM), which form the basis of production.

Presentations and sharings in an interdisciplinary content,

104 OLOGY

Aerology, Military Science (Army Science), Allergology, Algology, Andrology, Anesthesiology, Angiology, Anthropology, Atmology, Atomology, Bacteriology, Biogeomorphology, Bioclimatology, Biology, Biometeorology, Bioseology, Dosology, Ecohydrology, Ecology, Electrophysiology, Epidemiology, Eschatology, Etiology, Physiology, Gynecology, Histology, Histopathology, Hydrology, Immunology, Geobiology, Geology, Karyology, Criminology (veya Killology), Climatology, Kinesiology, Lagomorphology (veya Conyology), Chorology, Cryptology, Ludology, Mereology, Meteorology, Metrology, Methodology, Microbiology, Micrology, Mineralogy, Myology, Nanotechnology, Nephology, Neurology, Neuropathology, Numerology, Audiology, Ophthalmology, (Oxology), Ontology, Oncology, Orology, Osteology, Otolaryngology, Oceanography, Otorhinolaryngology, Parasitology, Pathology, Pedology, Penology, Personology, Petrology, Pyrology, Pneumology, Posology, (Patomology), Psychobiology, Psychophysiology, Psychology, Psychoneuroendocrinology, Psychoneuroimmunology, Pulmonology, Radiology, Reflexology, Rheology, Rhinology, Rheumatology, Symbology, Semiology, Serology, Sociology, Somnology, Sitology, Splanchnology, Stomatology, Thanatology, Teratology, Thermology, Typology, Topology, Toxicology, Traumatology, Tribology, Trichology, Vaccinology, Visserology, Virology, Zymology.

MOST USED WORDS

#artificialintelligence
#unmannedaerialvehicle
#maintenance
#sustainability
#realtime
#autonomoussystems
#cyber
#joint
#commandcontrol
#human
#adaptation
#technology
#informatics
#analysis
#speed
#robotics
#security
#strategy
#logistics
#digitaltwin
#sensor
#collaboration
#electronicwarfare
#machinelearning
#datamanagement
#energy
#ally
#decision
#design
#psychology

EXECUTIVE SUMMARY

The Future Soldier 2024 organization was held with the participation of representatives from domestic and international universities, research institutions, manufacturing companies, defence industry consultants, and firms operating in our country. The final report of the Future Soldier 2024 event, which took place on November 26-27, 2024, is presented in two sections: "Technology" and "Individual Soldier."

Topics such as Artificial Intelligence (AI), the Internet of Things (IoT), Big Data, Human-Machine Learning, Autonomous and Robotic Systems, Cybersecurity, Sensors and Electronic Warfare, Portable and Wearable Systems, Satellites and Space, and Quantum Infrastructure were presented under the "Technology" section, while human-centered approaches were addressed under the "Individual Soldier" section.

The analysis of advancements in military technologies was supported by examples from current events such as the Ukraine-Russia conflict, the Karabakh War, the Israel-Palestine clashes, the U.S.-China technology competition, and NATO and European Union initiatives. Experts in the field shared their insights, lessons learned, and future projections regarding these developments.

The importance of assessing the risks and opportunities associated with the development and use of new technologies in the short, medium, and long term was emphasized. For instance, it was highlighted that the rapid establishment of a national AI language is of great importance for national security, defence, and intelligence. Additionally, the need for active national and international involvement in addressing the ethical challenges posed by AI and the necessity of adopting a national strategy to develop early measures against AI-related risks were underscored.

It was also noted that converting big data into actionable intelligence would be one of the most significant force multipliers, while quantum technologies and blockchain are expected to offer major advantages in processing large datasets.

It has been concluded that data sharing plays a critical role in the development of new technologies, particularly in AI training and the enhancement of algorithms in autonomous systems. Establishing a structured data-sharing framework between the public and private sectors for software and technology development is seen as highly beneficial.

It was emphasized that in military defence technologies, the use of electronic warfare, cyber attacks, autonomous technologies, and robotics across air, land, sea, cyber, and space platforms as a "joint force" will continue to increase, with speed being a decisive factor. Additionally, the growing demand for interoperable, modular, lightweight, and easy-to-transport systems that do not restrict user mobility or increase cognitive load was highlighted.

The importance of communication systems, satellite, and connectivity technologies in both defensive and offensive military operations was underscored. Furthermore, munition technologies, swarm operations, and laser systems were identified as key force multipliers. It was also noted that deception technologies and digital twin concepts have the potential to reshape warfare doctrines, emphasizing the need to enhance data security measures in command and control systems. Special attention was given to the necessity of establishing cybersecurity as an institutional culture.

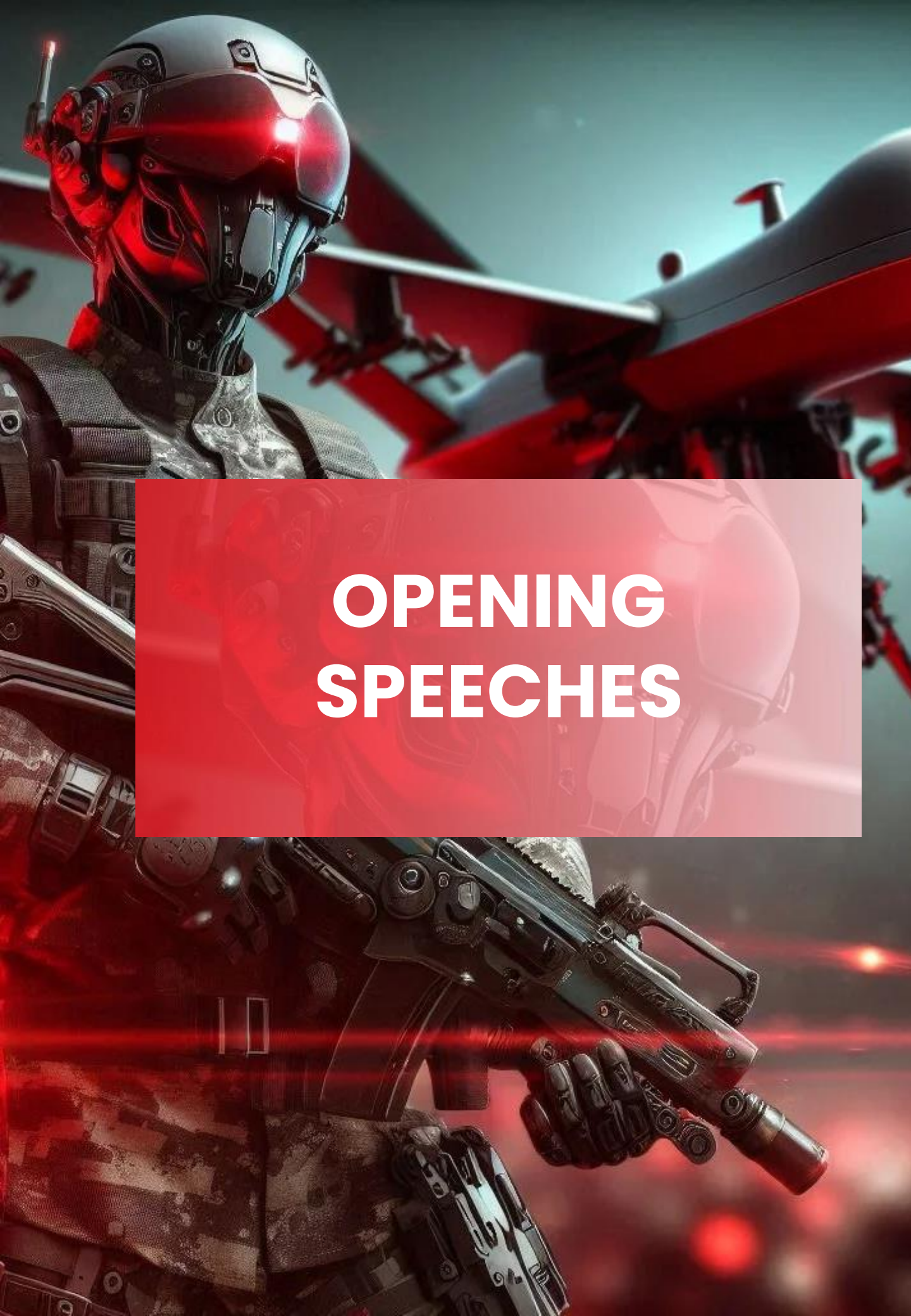
Participants stressed that humans remain at the center of all technologies, highlighting the increasing importance of training and skilled personnel.

Key topics discussed in the sessions have been included in the "Summary" section, while noteworthy statements from speakers are provided in the "Between the Lines" section. A comprehensive summary and evaluation report on all panel discussions has also been presented for your review.

Best Regards,

Oğuz HAMŞİOĞLU (PhD.)

SASAD Secretary General



OPENING SPEECHES

Osman OKYAY

SASAD Chairman Of The Board

Distinguished Commanders, esteemed representatives of our public institutions and organizations and sector companies, all distinguished speakers and participants, I greet you all with respect. Today, we have come together here at our event organized to evaluate the trends in global defence technologies.

This organization is not only an event where technological solutions are exhibited but today's rapidly changing security is an important platform that provides an opportunity to think about the importance of strategic planning and defence innovation.

Our vision, which brings together our armed forces and allies with the goal of enhancing next-generation combat capabilities, will hopefully serve as a guiding framework for our defence and aerospace industry. We are pleased to be hosting the third edition of this event alongside our valued stakeholders, following the inaugural event in 2008 and the second one in 2021, which took place despite the challenges of the pandemic and saw high participation. Once again, I extend my respectful greetings to all of you. To define the Future Soldier and the wars of tomorrow and to build our strategies accordingly, we must first gain a deep understanding of the challenging geopolitical landscape we currently face. In today's world, we are witnessing the rapid evolution of the international system into a multipolar competition, where major powers are intensifying their economic, military, and digital rivalries. However, this power struggle is not limited to leading nations—it is also shaping the geopolitical dynamics of middle-power countries with significant regional influence.

The ongoing Russia-Ukraine war in Eastern Europe continues to shake geopolitical balances, while China's growing military and economic influence in the Pacific, and the United States' evolving security strategies in response, signal new global tensions on the horizon.

The growing conflict in the Middle East, with its humanitarian devastation and moral burden, has the potential

to transcend regional security parameters and pose greater security threats. Israel's irresponsible escalation and expansion of its military campaign despite massive civilian casualties on the one hand, and Iran's growing military capability and aggression on the other, point to two major fundamental security challenges in the Middle East. On the economic front, trade wars and increasing protectionist policies impose serious regulatory and financial uncertainties on countries, especially in the areas of high technology, energy and raw materials. This has a profound impact not only on inter-state relations but also on export-oriented producers and industrialists, particularly those sensitive to global supply chain risks.

As a dimension of cyber security and military operations, cyber warfare and information operations have a significant place in an increasingly dangerous global security environment. While cyberspace has become an arena where non-state actors and state-sponsored groups can exploit security vulnerabilities, the rapid spread of information operations increases the security risks of countries in both domestic and foreign policy. In addition, factors such as climate change-induced security problems, decreasing resilience to disasters and weakening economic structures expand the dimensions of the concept of security. In light of all these uncertainties, Turkiye has been and will continue to take decisive steps to expand its strategic sphere of influence and strengthen its national security by producing its own products in the defence industry and building a high-tech infrastructure.
In this context, I believe that our efforts here are of great value, both in terms of strengthening the cooperation of our defence industry with allied countries and reinforcing Turkey's strategic role in the global arena.

The goal of expanding our strategic room for maneuver in the international system is the North Star of this route. Our defence industry eco-system, which we will reinforce by contributing to our allies through various diplomatic, military and commercial means, will make Turkey a leading actor in many global agendas beyond being a regional power in an era of global uncertainties.

Our event is of great importance not only for showcasing innovative technologies, but also for assessing the geopolitical implications of these technologies. Through the discussions and solutions presented here, we will focus on the technological trends shaping the future warfare environment and discuss Turkiye's leadership goals in these areas.

Throughout the event, we will have the opportunity to review our steps to further strengthen our country's role in global security together with the different stakeholders of our defence industry eco-system. I have no doubt that we will provide valuable inputs to our eco-system while discussing a wide range of topics from autonomous and robotic systems to wearable technologies, artificial intelligence and cyber security to energy security. It should be noted that the breakthroughs in our defence industry not only strengthen Turkiye's deterrence capacity, but also accelerate our integration into the global defence ecosystem. In this context, we see that the advanced technologies developed by Turkish industrialists not only provide operational superiority, but also become an innovation platform that brings together civilian and military fields with solutions that have dual-use potential. The effective use of these technologies will support our country to achieve a strategic position not only in the regional but also in the global security architecture.

The vision and cooperation we exhibit here today are the cornerstones of Turkiye's rising success in the defence industry. Your contributions will not only put our country at the forefront with its production power, but also with its strategic leadership in the global arena. I sincerely believe that our event will be an inspiring and collaborative platform. I would like to thank all our participating stakeholders again and wish you a useful event.

Best regards.

Lieutenant-General Zorlu TOPALOĞLU

Land Forces Command Commander of Training and Doctrine (EDOK)

Mr. Chairman,
Esteemed comrades-in-arms, distinguished representatives of public institutions and our defence industry, valued participants from both home and abroad,I would like to begin my remarks by extending my deepest condolences to the citizens who were martyred in the heinous terrorist attack on TUSAŞ, the pride of the Turkish defence industry, on October 23, 2024. May Allah grant them mercy, and I also wish a speedy recovery to the dedicated employees of TUSAŞ who were affected by this tragic event.

I am delighted to be with you at the International Future Soldier Conference, organized by SASAD, where end users, procurement authorities, manufacturers, and research institutions come together.I firmly believe that such events, which bring the Turkish Armed Forces together with public institutions and domestic and international defence industry organizations, will contribute significantly to shaping the future security landscape and fostering greater international cooperation.

Distinguished guests, distinguished participants,

In order to become a strong, deterrent and effective army, it is of utmost importance not only to be able to keep up with technology, but also to go one step beyond it and aim to pioneer modern technology, to base its vision on sound and scientific concepts in order to achieve this goal, and to produce new weapon systems that other world armies do not have.

Developing technology and emerging innovations, especially rapid developments in areas such as artificial intelligence, autonomous systems, hypersonic systems, quantum sensors and nanotechnology such as biotechnology, are affecting and changing the way of warfare, concepts and doctrines. Moreover, these developments are bringing about fundamental changes in the defence and security sector.

In the battlefield of the future, AI-powered analysis and decision-making systems will enable instant and accurate

decision-making, while autonomous systems will minimize human involvement, reducing risks and enhancing operational effectiveness. Beyond technological advancements, ethical responsibility and sustainability will also be fundamental pillars of future military structures. Weapon systems must be developed with a focus on environmental impact, ensuring that sustainable and eco-friendly solutions are integrated into military operations.

Furthermore, establishing ethical and legal regulations regarding the use of AI in warfare is of critical importance for ensuring the protection of human rights. Steps in this direction must be taken with a proactive approach and a comprehensive understanding. Global threats and security challenges are not issues that any single country can overcome alone. Therefore, international cooperation, information and technology sharing, joint training and exercises, and interoperability efforts will be essential in strengthening collective security and ensuring lasting peace. On the other hand, no matter how advanced technology becomes, the human factor will always remain the most crucial element. While future soldiers will be equipped with the capabilities offered by advanced technology, it is clear that—just as in the past and present—decisive outcomes in combat will ultimately depend on well-trained personnel. Future soldiers must not only possess the knowledge and skills to adapt to cutting-edge technology but also cultivate ethical values and leadership qualities. In this regard, modernizing our training systems and ensuring the continuous development of our military personnel will be of vital importance.

No matter how advanced a soldier's weapons and equipment become, the ultimate decision-maker in the battlefield of the future will still be the human. With this reality in mind, it is essential to train future soldiers comprehensively in areas such as technology and cybersecurity, hybrid warfare, unmanned aerial, ground, and naval vehicles, autonomous systems, simulation and virtual reality, intelligence and analytical skills, psychological resilience, rapid and accurate decision-making, competence, and human management. As technology evolves, the variety and impact of threats on the battlefield continue to grow each day. Consequently, the scope of soldiers' responsibilities is expanding and their operational

influence is increasing.

In this context, in order to increase the effectiveness of both survivability measures and the missions carried out, the equipment used by the military must also be developed to adapt to the missions performed. The types of equipment that the soldier of the future should have can be listed and summarized as follows:

Personal protection equipment, communication and information systems, cyber and electronic warfare equipment, weapon systems, tools and systems that affect maneuverability and logistics, new generation concealment and cover technologies that prevent their detection by the enemy, and deception technology are the most important ones. The design of these technologies should be capable of meeting the mental and physical needs of the soldier in a combat environment. The measures to be taken in situations that do not require the soldier to make a decision, especially for survival measures, should be realized autonomously. With in the scope of the training of personnel, virtual and augmented reality technologies that will enable them to continue their training in any environment where Tek-Er is present, including operational intervals, and software and hardware that will provide support as if they were moving in a real environment should be used. Situational awareness should be increased through the visualization of big data. These applications will also facilitate the control of other decision and support systems to be used with combat and information systems.

Advances in computer technologies should be able to identify missions and possible courses of action to address threats, enabling the soldier to make situational judgments and decisions, and to communicate these decisions simultaneously to personnel identified in the system. The systems should be able to recognize the friendly criteria defined for its own personnel, and should automatically deactivate in the event that they fall into the hands of the enemy. For this purpose, it is important to develop lightweight, practical and ergonomic equipment that will increase the soldier's mobility and maneuverability and provide protection. Therefore, it is of great importance to develop survivability measures in the face of ever-increasing threats on the battlefield.

Every soldier must be able to continue his duty without being affected by all kinds of combat and climatic conditions. One of the most important factors in the victories of our ancestors, which started in Central Asia and embellished Turkish history, has been the ability of soldiers to move agile and swiftly. In order for Tek-Er to maintain its combat and survivability capability, the energy required by the logistics system and equipment for these systems must also be practical, fast and uninterrupted. One of the most important factors in the command and control of unmanned systems will be the human-machine interface. The commander's operational design should be able to be transferred to unmanned systems without speaking. Since a security vulnerability at this point could lead to unmanned systems that can be electronically captured and used against our troops, the protection and security factor comes to the fore. In this context, there is also a need for the development of Tek-Er systems with high situational awareness, survivability, fire and maneuver capability, which can undertake missions in the battlefield of the future both as a unified system and as a stand-alone system, and for evaluations to be made to ensure the integration of these systems with other systems in the battlefield.

Dear participants, I believe that the two-day 'International Future Soldier'24' Conference will be beneficial in terms of following the studies, technological developments and future predictions in this field, revealing the capabilities of the defence industry and raising awareness. We respect the territorial integrity of our neighbours and are in favour of dialogue within the scope of the principle of 'Peace at Home, Peace in the World' as expressed by the eternal commander-in-chief Gazi Mustafa Kemal Atatürk. However, we are also determined to protect the rights, laws and interests of our country. The effectiveness, deterrence and prestige of the Turkish Armed Forces, which has gained great capability and experience in the fight against terrorism, is a great gain for our friends. I would like to emphasize that we are ready, within the framework of the legislation, for all kinds of information needs and requests for joint work in the development of the capabilities of the Turkish Armed Forces.

I hope this conference proves to be productive for all participants and extend my sincere regards.

BETWEEN THE LINES

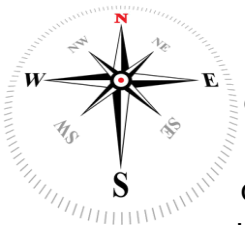
TECHNOLOGY IN TODAY'S CONFLICTS

Autonomous Systems and Unmanned Aerial Vehicles have a decisive impact on the course of war by targeting enemy defence lines and gaining strategic superiority.

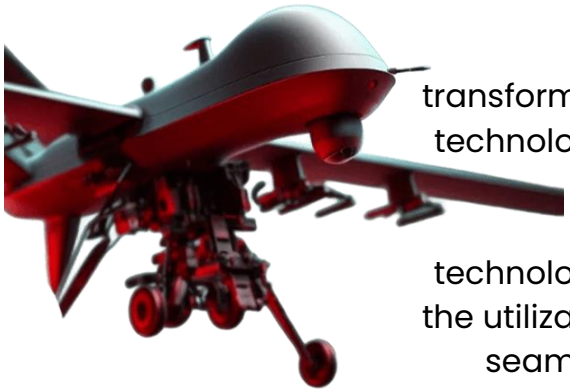
Ukraine initially secured a notable advantage over Russia during the war's onset through the deployment of the TB2 Bayraktar. However, it became evident that the Russians rapidly adapted to counter this. The critical aspect lies in the sustained rate of innovation. The battlefield is witnessing an astonishingly rapid pace of innovation, driven by the private sector and emerging ventures.

The ongoing conflict between Ukraine and Russia has further highlighted that modern warfare hinges on understanding the adversary's objectives. In this context, the aerial perspective offered by Unmanned Aerial Vehicles (UAVs) is paramount for gaining detailed insights and adapting combat strategies.

The unique moment that started with the Baykar TB2, which was initiated by countries with their own production and technology chains, can be called a 'flare, spark or sparks'.
The ability of this spark to create its own cycle, to continue and turn into a fire, to go further and achieve permanence, and to build its own independent military industry is a turning point in the destiny of countries and nations.



The role of the TB2 Bayraktar in the Ukraine-Russia conflict has signaled a pivotal shift, demonstrating the disruption of technology monopolies, the erosion of traditional powers' exclusive production capabilities, and the increased capacity of other nations to influence geo-economic and geopolitical landscapes.



The conflict between Ukraine and Russia has transformed into a critical testing ground for technology firms. Beyond trials across Land, Air, Sea, Cyber, and Space, this war has yielded vital insights into technological rivalries, resource acquisition, the utilization of low Earth orbit technologies, seamless communication networks, and industrial innovations.

These experiences are compelling a reassessment of strategies and doctrines, spanning economic policy to command centers and influencing technological leadership, while also refining aspects like situational awareness, tactical approaches, information governance, and military coordination.

Ukraine's human resources, industrial capacity, and the economic support of NATO countries are preventing Ukraine from making sustainable progress and being effective in frontline battles. They are developing their own concepts where Unmanned Aerial Vehicles (UAVs) can replace artillery weapons and annihilate Russians in positional warfare. For example, they are also trying to counter electronic warfare with fiber drones.

In the Ukraine-Russia War, the measures taken to protect tanks from FPV unmanned aerial vehicles by bringing a technique from the Assyrians dating back to 2000 BC to the 21st century demonstrates the importance of simple but clever methods for strong defence and fewer casualties. This should also make us think about powerful munitions in terms of making strong armored tanks or how to penetrate them if our opponent does so. We should also consider how tanks prepared for the classical warfare environment are destroyed in the fast-paced battlefield or how they are protected with simple ingenuity.

In the Ukraine-Russia War, the Russian tactic called the **'Pinpoint Strike Point and Crank Concept'** is admired by all war experts, including the Americans. The advance of the Russian reserves on the Orikhiv, Kurakhov and Kurshcyna lines, where they were expected to face logistics and supply problems, surprised everyone. We see that they are taking very effective measures with aerial imagery and electronic warfare data, using new technologies not only for killing but also for sustainable warfare, and mobilizing these technologies in terms of using their supply forces. The unit, which has independence and autonomy in conducting its own operations and is responsible for about 300 square kilometers, directs the war as it pleases, luring Ukrainian soldiers to the areas they want and making pinpoint strikes in these areas.

Polish and European war experts believe that the Russians are advancing 30-kilometer-long lines with special units using pinpoint strikes, both longitudinally and transversely.
Creating a circular motion like a 'crank', the Russians manage a kind of machine advance with artillery batteries, electronic warfare and unmanned combat vehicles. Their big smart bombs also help the advance.

We are also seeing the impact of 'Battery' units, the smallest artillery units in the army, on the Russian advance. Especially in the South, we observe that the Russians are advancing in 10-kilometer sections using unmanned aerial vehicles and especially FPV drones. We see that they prepare 'Battery Units' every 10 kilometers for a new offensive, and then advance with the support of FPV drones and artillery fire after surveillance with satellite and unmanned reconnaissance vehicles.

It is imperative that logistics in wars be designed in periods according to new technologies and the development of these technologies.

Azerbaijan's effective use of UAVs and UCAVs to target enemy defence lines and gain strategic superiority highlights the importance of modern technologies in military operations, while also demonstrating the impact of safer and more coordinated work.

A new technology entering the battlefield does not mean the disappearance of previous dynamics. For Europeans, if you had said 10 years ago that there would be a war between Ukraine and Russia resembling a World War, no one would have believed it. So what happened? You see trench warfare similar to World War I. Drones make the battlefield visible for the infantry soldier and clear the front line. But you still need ammunition. You create new dynamics on the battlefield by combining this with developing technologies.

We are also seeing the impact of 'Battery' units, the smallest artillery units in the army, on the Russian advance. Especially in the South, we observe that the Russians are advancing in 10-kilometer sections using unmanned aerial vehicles and especially FPV drones. We see that they prepare 'Battery Units' every 10 kilometers for a new offensive, and then advance with the support of FPV drones and artillery fire after surveillance with satellite and unmanned reconnaissance vehicles.

The conflicts in Ukraine and Gaza have become extraordinary testbeds for artificial intelligence and autonomous systems. These theaters are providing critical insights into how civilian-oriented technologies are being repurposed for military applications. For instance, ride-hailing apps, designed to connect passengers with taxis, have been adapted to facilitate artillery strikes and drone reconnaissance coordination for Ukrainian civilians.

AI

We see that data obtained from open-source and seemingly innocent technologies results in the bombing of cities' electricity distribution centers, ammunition shipments, or centers, with the aid of artificial intelligence. Electronic jamming systems and electronic warfare have brought about the transition from GPS systems to fiber systems in FPVs, or autonomous mission completion with artificial intelligence support.

We are seeing the first signs of robot warfare in conflict environments with unmanned land and sea systems.

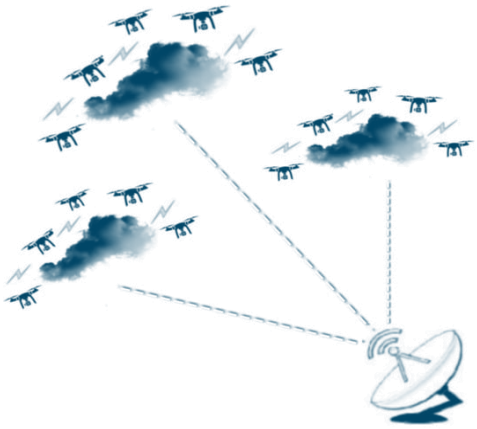
And we are moving from the use of small robots to the use of large robots.

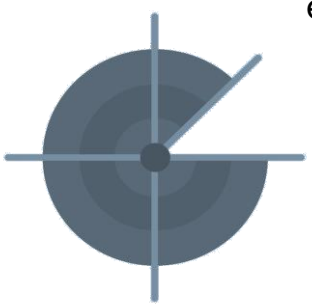
The transformation of commercially available drones into weaponized platforms, such as those used by ISIS in 2017 to inflict weekly casualties of approximately 30 Iraqi soldiers with AK-47 attachments, and their subsequent evolution into precision-guided munitions or kamikaze drones, underscores the swift technological advancements shaping modern warfare and the emergence of novel combat landscapes

Russia's carrying of thermobaric payloads (vacuum bombs) with Shaid 36 Unmanned Aerial Vehicles, and targeting shelters in Odessa, is a lesson in the lethal and high-impact dimensions of new technologies.

The Russia-Ukraine conflict is the most recent example of the state of technological conflict. It is also redefining how wars are fought, lost or won.

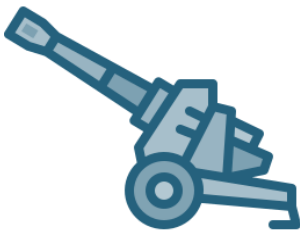
We are seeing many new tactics on the field, such as target deception systems that confuse armed unmanned aerial vehicles with fake unmanned aerial vehicles, the use of unarmed decoy drones designed to mimic the radar signature of armed aerial vehicles and prepared to impact the air defence system, and making it difficult to distinguish between different types of threats.

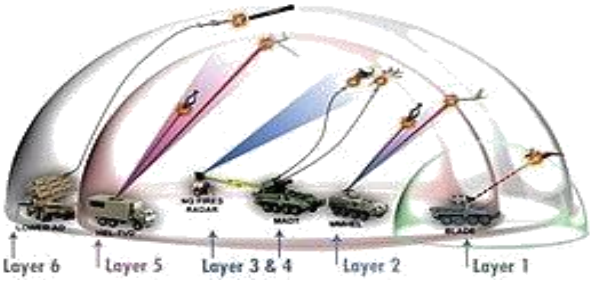




The Ukraine-Russia war has been a fresh example of incorporating artificial intelligence systems into the analysis and rapid decision cycle in a conflict environment. Artificial intelligence was utilized to observe, direct, make decisions, and take preemptive measures before the enemy acted, using imagery from satellite and reconnaissance vehicles.

Hypersonic missiles, anti-technology missiles have revolutionized artillery with the ability to fire pinpoint strikes with smart technologies, long hitting range and effective damage.





Ukraine the conflicts in Ukraine, neither side has been able to gain superiority due to the failure to establish air superiority and the limited effectiveness of ground operations. It is predicted that there is no clear superiority in the war because this superiority cannot be established despite the parties firing missiles and rockets at each other.

BETWEEN THE LINES

ARTIFICAL INTELLIGENCE

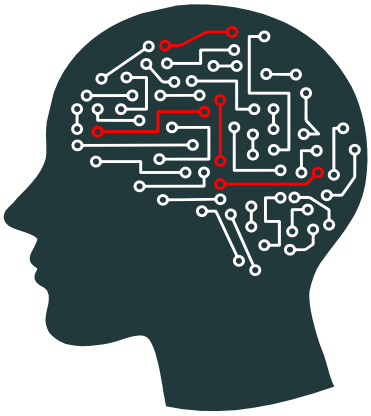
The core strength of artificial intelligence lies in its capacity to break down and analyze data, a task at which it is exceptionally proficient. In contemporary society, its most significant role in both civilian life and military applications is as an analytical enabler.

Information warfare is a longstanding practice, dating back to the Roman Empire, with only the methods evolving over time. While artificial intelligence is often perceived as a disruptive force, we must recognize its capacity for scalability and quantifiable impact in modern information operations.

Despite concerns and risks, there are numerous opportunities in artificial intelligence. A research and development (R&D) and product development (P&D) structure based on short, medium, and long-term opportunities and risks in technologies used in both civilian and military dimensions will ensure the healthy management of labor, value, and time planning.

Strategic imperative dictates that authorized entities undertake comprehensive studies across diverse working groups to analyze artificial intelligence trends, probabilities, impacts, periods of uncertainty, and potential action plans. This includes delineating the military AI ecosystem and distinguishing between allied and adversarial systems. Furthermore, meticulous planning is essential to categorize data according to its significance, without the necessity of establishing a centralized data repository.

Information warfare is a longstanding practice, dating back to the Roman Empire, with only the methods evolving over time. While artificial intelligence is often perceived as a disruptive force, we must recognize its capacity for scalability and quantifiable impact in modern information operations.



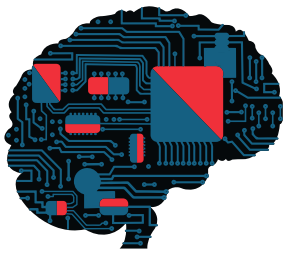
In the immediate future, military platforms enhanced by artificial intelligence will prioritize the synergy between human-machine collaboration and infrastructural strengths. Military AI is set to evolve into an increasingly potent force multiplier.

Military artificial intelligence presents both opportunities and strategic targets for capabilities within the Command, Control, Communications, Computers, and Intelligence (C4I) framework, specifically concerning adversarial forces. AI possesses a myriad of potential applications across all facets of defence. The integration of AI technologies will be indispensable in various domains, including intelligence analysis, decision support systems, war gaming, simulation, electronic warfare, unmanned, robotic, and swarm systems, optimization of both general and field logistics, development of military proficiencies, operational deployment, and the establishment of a robust, sustainable economic model.

If new mechanisms are not introduced into the competition over military artificial intelligence, the super rivalry between the US and China could become destabilized, and this could become a threat to other nations.

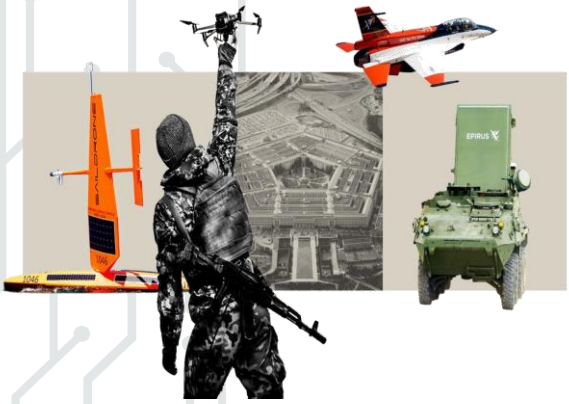
Artificial intelligence and its military use provide the development and potential of different production and product capacities for democratic and authoritarian regimes

The global governance of military AI puts small states at risk of being left behind by larger players.

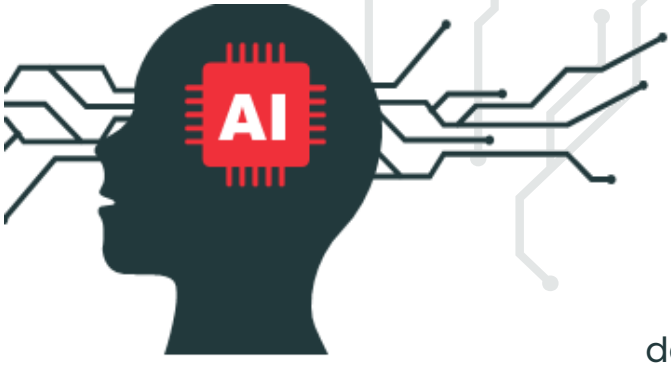


NATO and the West should closely monitor the artificial intelligence programs of countries such as Russia and China, and develop programs that can counter their use in modern warfare and intelligence.

The trajectory of artificial intelligence development is influenced by numerous factors beyond the direct purview of NATO and Western powers. A collaborative and inclusive strategy, encompassing allies, partner nations, industry stakeholders, academic institutions, and civil society organizations, is essential to effectively advance military artificial intelligence capabilities.



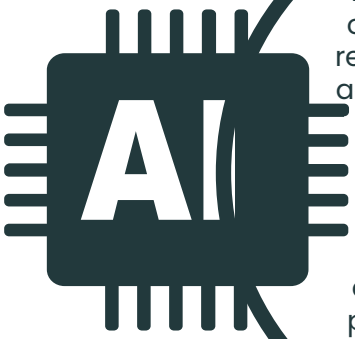
Informed and artificially intelligent warfare' may be among the new terms in military literature.



Artificial intelligence also presents new and different threats and opportunities for non-governmental organizations (NGOs).

China has focused on areas such as artificial intelligence-centered combat intelligence systems and counter-system destruction, cognitive domain destruction, and the like. It is trying to carry out studies focused on winning without fighting by triggering decision-making and system paralysis through cognitive warfare.

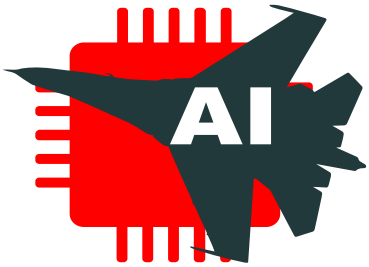
The global military and political landscape is undergoing transformation due to the proliferation of intelligent, autonomous, and semi-robotic systems. These systems are assuming a pivotal role in shaping the influence and capabilities of nations.



AI presents significant opportunities and risks related to influencing an adversary's perceptions, disrupting their information domain access and cognitive processes, creating disorder, neutralizing counter-systems, and paralyzing command-and-control infrastructure.

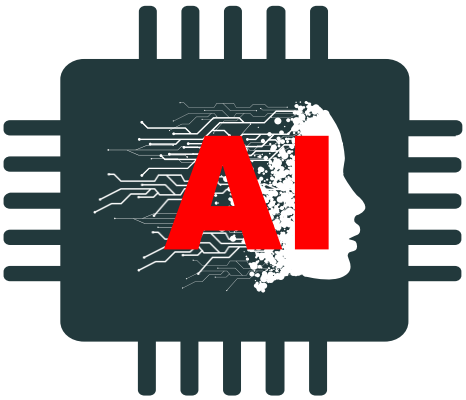
Artificial intelligence systems, together with the sub-technologies they will use, will determine the multiplier effect on war capabilities with their data analysis, speed, location and lethality.

In the event of a collapse of artificial intelligence systems, the continuity of being able to revert to non-artificial intelligence-dependent systems will be among the most important advantages. This is also considered an example for the resilience and emergency preparedness of armies worldwide.



The US Army Air Force announced that an artificial intelligence algorithm can fly a jet and autonomously perform 8 different tasks. Due to artificial intelligence working faster than us, we must consider how to integrate growing autonomy with this kind of technology into industry and human resources.

New military structures based on autonomous, robotic, and artificial intelligence systems are inevitable.

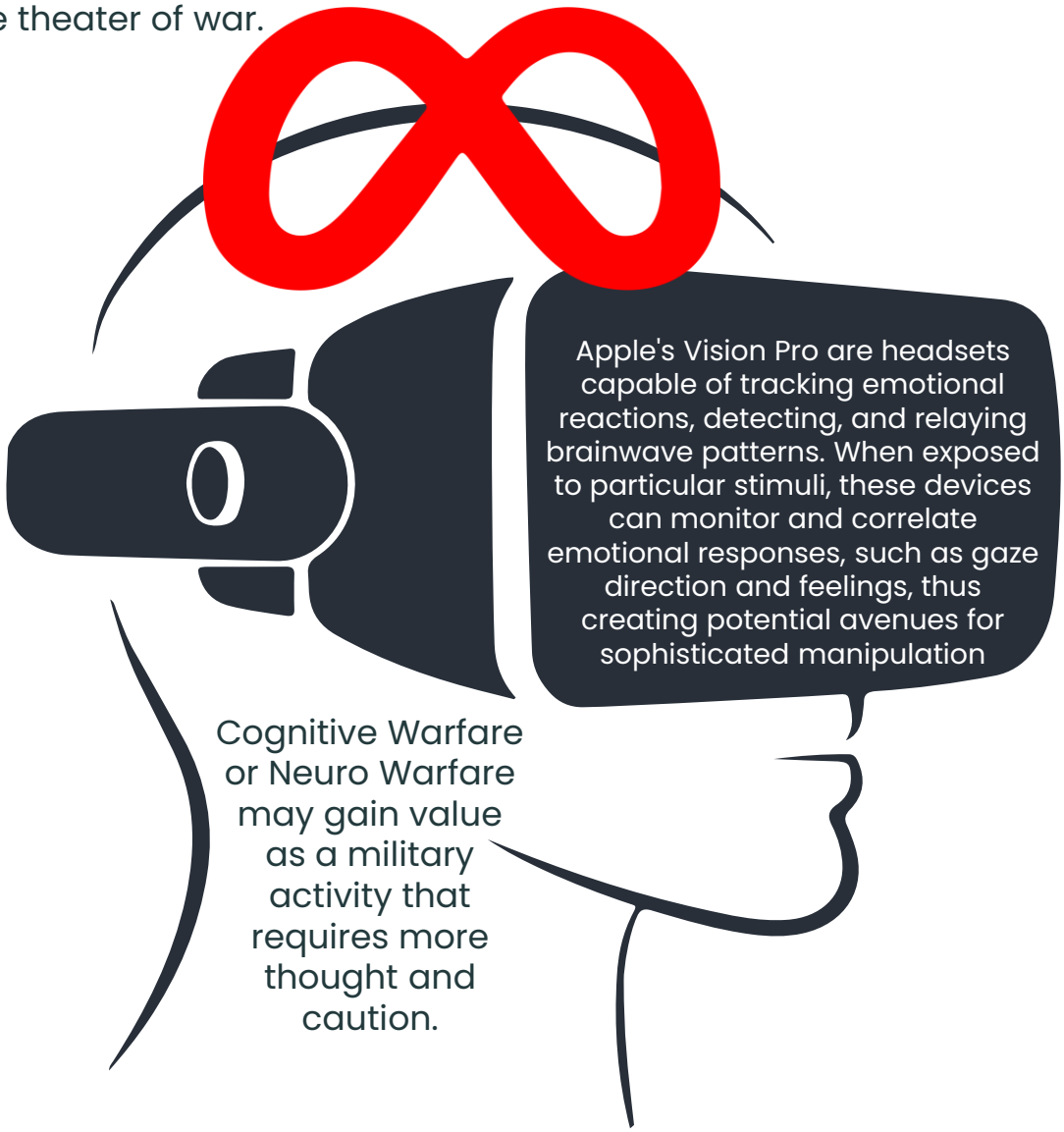


Autonomous systems and unmanned aerial vehicles are creating new commands in the world's armies.

DeepFake, information and manipulation, political, economic and social disruption, and distorted military decision-making processes are the latest examples of the use of artificial intelligence technologies today and the dimensions of the threats they can pose.

The era of Cognitive Warfare is upon us. In this paradigm, the human mind becomes the primary battleground, as individuals are confined within curated information ecosystems that reshape their perceptions. Cognitive Warfare transcends mere information dissemination; it is a strategic endeavor aimed at manipulating not only the content of thought but also the very processes of cognition.

Deepfakes emerged in 2014, enabling the manipulation of images and videos. Their military application surfaced in March 2022, with a deepfake of President Zelensky urging Ukrainians to surrender, followed by a manipulated announcement of martial law by President Putin. These events triggered widespread panic. Had you asked me, as a military analyst in 2013, how this technology would influence mass behavior or warfare a decade later, I could not have predicted its impact. Understanding the operational dynamics of such nascent technologies in a combat scenario and mastering their application is crucial. This represents not only exponential technological advancement but also a significant evolution in the theater of war.



Deepfake technology facilitates the asymmetrical exploitation of inherent psychological biases within individuals

Artificial intelligence and human-machine collaboration have an incredible potential to create duality. You must carefully calculate how much to trust each and who will make the final decision.

The continued utilization of unmanned systems necessitates an augmented degree of autonomy, rather than a diminished one.

Artificial intelligence will operate in two separate paradigms: human-centered and technology-centered.

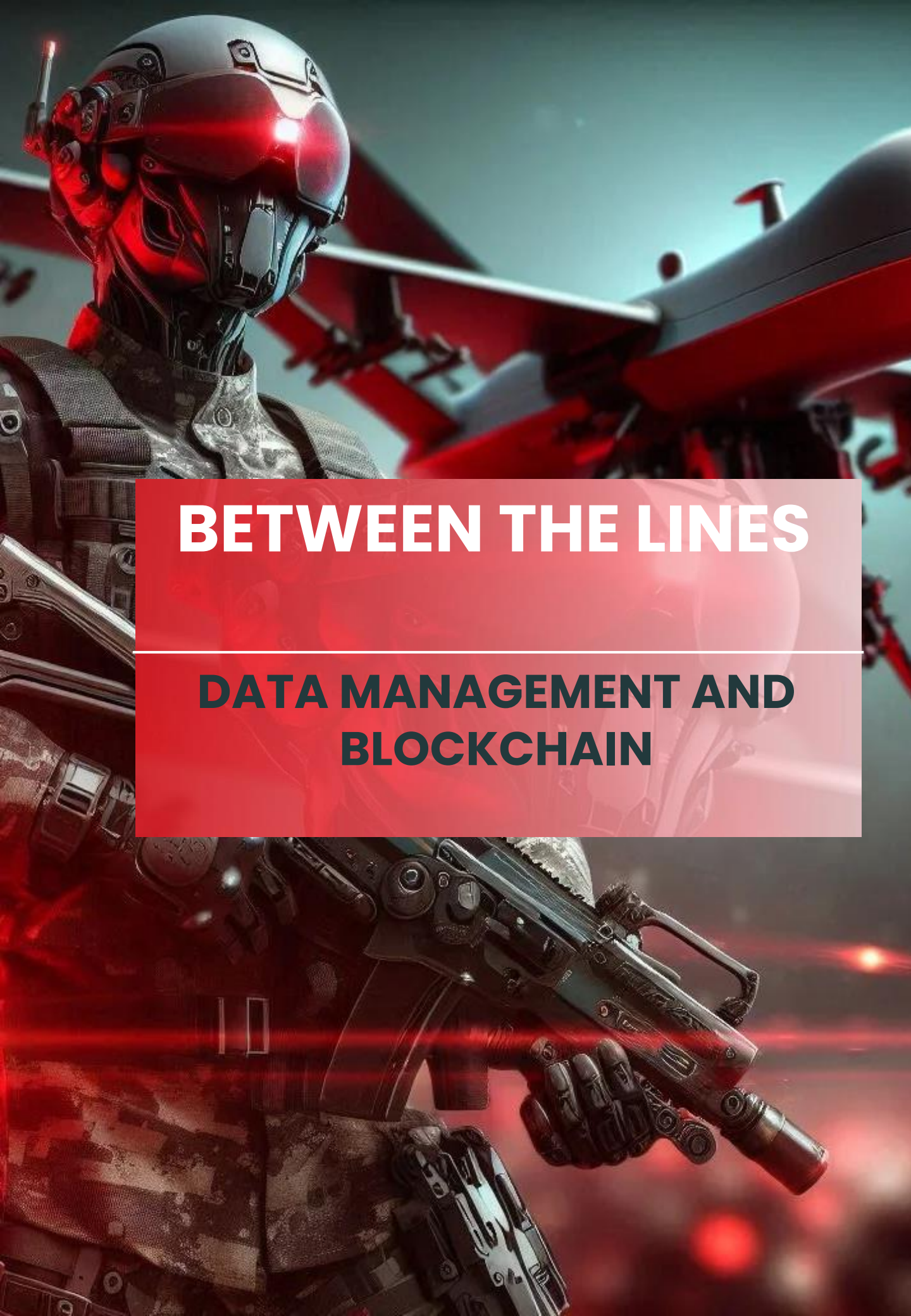
The critical question for artificial intelligence is; what do you want from artificial intelligence and what should it achieve? You cannot make a comparison without knowing and determining your strategic ambition level. If you don't have a benchmark or roadmap, you won't know what to follow and what to do.

We can clearly see the desire of most countries to use and combine artificial intelligence and unmanned systems together;
'shoot if it's a fighter or don't shoot if it's a civilian'.

DARPA makes two distinctions for artificial intelligence. The first wave of artificial intelligence is the machines implementing what humans have coded. The second wave of artificial intelligence is asking machines to make sense of this data. The third wave is to learn on its own how to learn artificial intelligence in the best way. They will be systems that understand each other in the context in which they operate, decide on the consequences of their own actions, and understand their results. More importantly from a military perspective, they will be systems that understand the consequences of hostile actions. Periods when decision-making authority is completely transferred to machines may be experienced here.

The initial periods of artificial intelligence use on the battlefield will be a period where humans are redesigned and advanced combat tools are redesigned. It will evolve into a period where human control is within, but human control may be phased out in decision cycles. Periods where humans adapt to and overcome a technologically enhanced conflict may be medium and long-term war strategies and environments.

Artificial intelligence functions as a tool, with humans as its directors. However, what are your objectives, and what specific tasks should artificial intelligence undertake?



BETWEEN THE LINES

DATA MANAGEMENT AND BLOCKCHAIN

Contemporary warfare is characterized by an immense volume of communication and data exchange. The transformation of raw data into actionable intelligence is a pivotal challenge in technological planning.

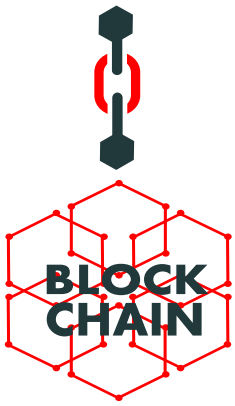
The efficacy of military technologies hinges on robust communication security, informed decision-making, and protected data dissemination. Blockchain technology, characterized by its distributed, decentralized, immutable, and transparent architecture, can bolster security and coordination for autonomous air power systems through its secure communication and effective coordination capabilities.

BLOCK CHAIN

Blockchain technology, with its distributed structure and the immutability of the entered data, can contribute to secure data flow. It offers great potential in the future in areas such as the storage and protection of confidential and critical information, the integrity and confidentiality of communication, and network-centric warfare.

Blockchain technology provides operational security solutions for the collection, analysis, secure storage, recording, and transmission of battlefield intelligence gathered by UAVs and comparable platforms.

The integration of artificial intelligence, big data, quantum, and blockchain can bring about major changes, changing the definition of cognitive power.



South Korea is developing initiatives to enhance the reliability of its autonomous robotic border defence systems through blockchain technology integration.

China is actively developing initiatives in blockchain-based identity management and provisioning for military robotics, aiming to counter manipulation-prone identity systems. By assigning each robot or unmanned system a distinct blockchain identity, ensuring operation solely within pre-authorized parameters, they guarantee control exclusively by authorized personnel..

Autonomous systems can quickly share intelligence on a common blockchain and enable the determination of strategies in dynamic combat environments. The US Air Force is testing real-time information sharing on the blockchain for autonomous drone swarms. These systems can attack targets more effectively by increasing coordination within the swarm.

Blockchain is a system with the power to reshape security doctrines and redefine geopolitical strategies by integrating air power with other domains such as space, cyberspace, land, air, and sea. In this respect, it has great contribution potential in coalition operations and cyber security priority.

Blockchain technology holds substantial promise for a wide array of military applications, particularly in the domain of big data processing.

BETWEEN THE LINES

CYBER, SPACE, AND ELECTRONIC WARFARE

Russia jammed GPS signals to disrupt Ukrainian navigation and targeting systems. Ukraine's drone counter-electronic warfare systems enabled it to disable Russian UAVs mid-flight. We also closely witnessed a new defence technology cycle for each attack.

Advancements in spectrum technology have necessitated the identification of security vulnerabilities, the detection of weaknesses, and the implementation of counter-technologies.

Cyberattacks orchestrated by Russian state-backed actors targeted Ukraine's vital infrastructure, encompassing power distribution networks and financial institutions. Notably, the assault on Ukraine's electrical grid was especially consequential.

The cyber domain is a site of constant activity, with operations in the realm of cyber warfare assuming paramount importance. These developments underscore the inextricable link between the digital and physical realms and their far-reaching implications. Consequently, the increasing prevalence of cyber warfare empowers even smaller nations to inflict substantial damage upon significantly more powerful adversaries.

Battlefields are evolving, transitioning from purely physical spaces to encompass information and cognitive domains. The significance of Command, Control, Communication, and Computers (C4) in modern warfare is experiencing an unprecedented surge.

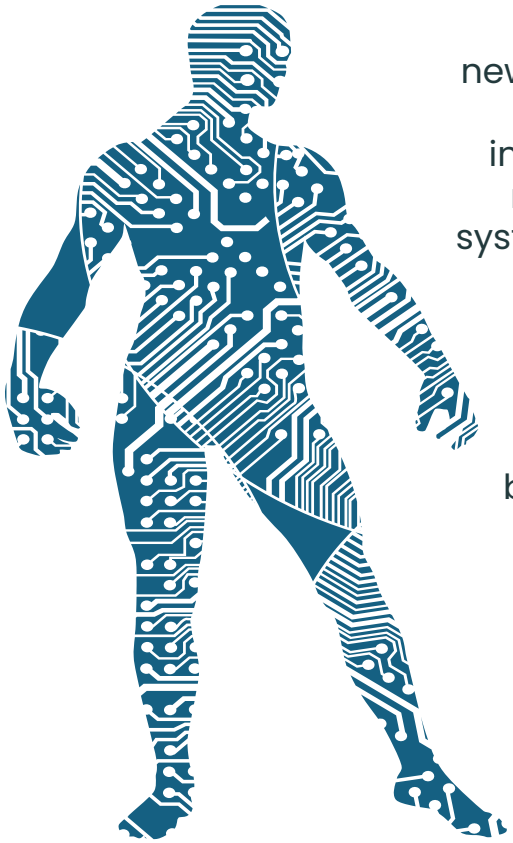
Advancements in technology are elevating electronic warfare to a paramount force multiplier. Vulnerability through the electromagnetic spectrum, coupled with the growing importance of space and cyber warfare, underscores this trend.

BETWEEN THE LINES

THE FUTURE SOLDIER AND EDUCATION

Advanced combat helmets incorporate augmented reality displays and provide soldiers with seamless data access. Equipped with these technologies, soldiers gain real-time battlefield intelligence, enabling them to access a wealth of information, including maps, threat assessments, and mission objectives, with minimal communication. This facilitates immediate situational awareness and expedited decision-making in combat scenarios. The United States Army, for instance, places significant emphasis on programs like integrated visual augmentation systems.

Nations are investing in exoskeleton technology to reduce fatigue and increase endurance. The Ukraine conflict has also revealed that this technology is vital in urban warfare scenarios.



The advent of new technologies does not instantaneously render existing systems obsolete. A pragmatic approach necessitates a balanced integration of both novel and established technologies.

Integrating more people into innovations and integrating machines with humans are also necessities of the new generation of warfare.

We are seeing signals that robotic systems will revolutionize battlefields, especially in human casualties, with the performance of land, sea, and air vehicles.

We must find a way to partner through human-machine mediation. We operate with a half or 1-second intelligence speed, but artificial intelligence operates at nano-speed. We must find a way to truly partner, to combine paths.

The influence of technology, both beneficia and detrimental, on military personnel must be carefully regulated. The development of physical and nutritional enhancements tailored to battlefield and combat environments, coupled with the design of corresponding training regimens, is of paramount significance.

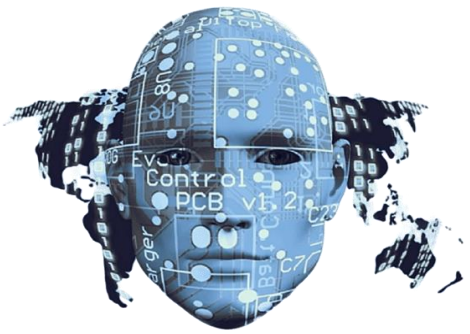
The development of any technology aimed at enhancing the soldier's mobility, agility, and operational efficiency in the field must prioritize usability and practical applicability. For the soldier, the paramount attribute is the rapidity of reaction.

NATO is placing significant emphasis on Multi-Domain Operations. In the imminent future, human involvement in fundamental decision-making processes will be somewhat reduced, with autonomous systems and machines handling routine decisions. However, high-impact, outcome-driven decisions will remain human-centric. Consequently, the concepts you highlighted, including autonomous decision-making, temporal frameworks, and the integration of human and unmanned systems, are subjects of intense deliberation within NATO. Machines will assume responsibility for minor decisions to alleviate the cognitive load on human operators. During the synchronized operation of land, sea, and air assets, it is anticipated that automated systems will make decisions, thereby minimizing the need for human intervention in intricate technical aspects.

Emerging technologies necessitate collaboration with more adaptable and resilient personnel. The integration of both novel and legacy systems will demand substantial coordination between historical and contemporary practices. Envisioning the military of the future may entail relinquishing established paradigms, setting aside familiar tools and methodologies, and embracing innovative approaches and strategies.

BETWEEN THE LINES

ETHICS, NATIONAL AND INTERNATIONAL COOPERATION

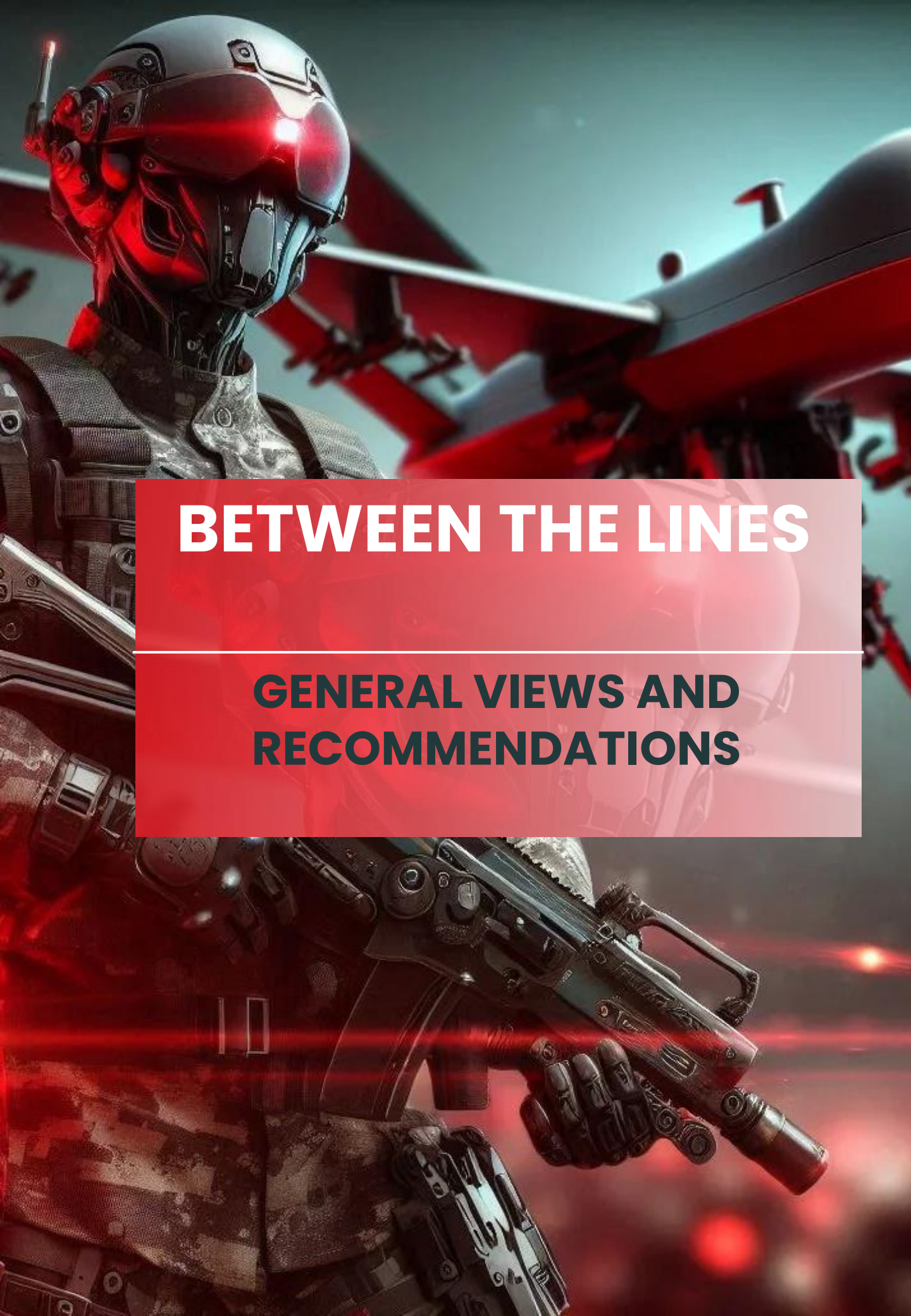


A preemptive strike in anticipation of a swarm attack risk constitutes a breach of Article 2, paragraph 4 of the United Nations (UN) Charter. The UN Charter does not recognize this action as prevention; indeed, this technology possesses the potential to fundamentally undermine established international UN norms.

NATO and Turkey are important players with a strong artificial intelligence industry and academic research base. This means that NATO allies have the opportunity to take advantage of the early stages of artificial intelligence and solidify this process.

The increasing intelligence of machines elicits significant ethical apprehensions. While the potential for both widespread casualties and life-saving interventions exists, it also raises concerns regarding accountability.

The democratization of technological access and the proliferation of technological autonomy give rise to profound ethical dilemmas regarding the application, misuse, and malevolent exploitation of nascent technologies. Furthermore, the integration of human and machine, or human-machine convergence, will inevitably provoke intricate philosophical inquiries into the very essence of humanity.

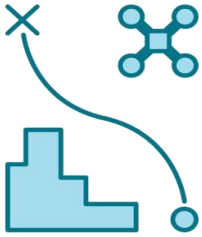


BETWEEN THE LINES

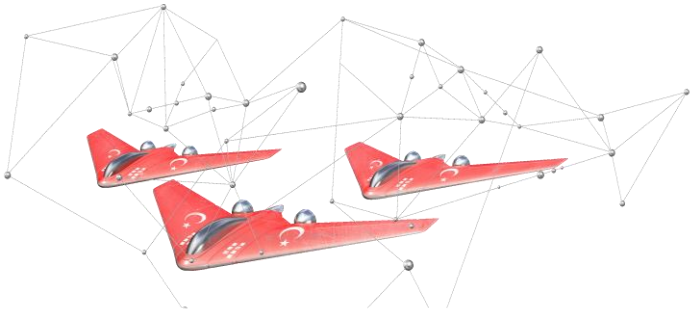
GENERAL VIEWS AND RECOMMENDATIONS

To prevail in the conflicts of tomorrow with the warriors of tomorrow, true strategic acumen is essential. While artificial intelligence, cloud computing, autonomous systems, and real-time strategy simulations will prove invaluable, ultimately, sound judgment will dictate the outcome. The judicious deployment of available resources at critical junctures by those in command will be the decisive factor.

War is understood as a 'test laboratory' for the capabilities of dual-use technologies.

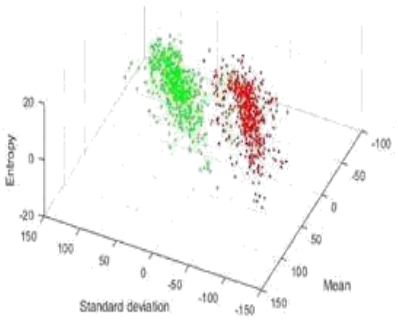


Emerging technologies are revolutionizing military techniques, tactics, and the engagement sequence. The age-old combat doctrines of 'locate, suppress, encircle, close, and eliminate' are undergoing a profound transformation.



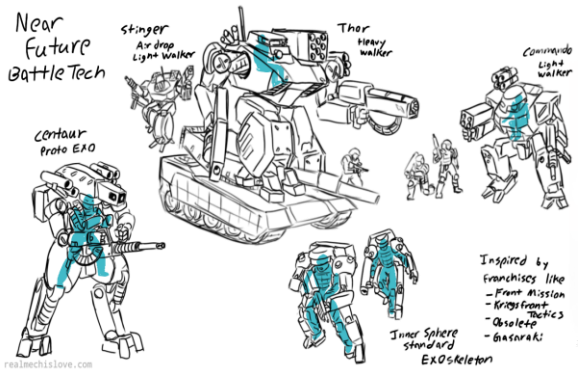
In bird flocks, no individual bird is aware of the shape they form; it's like a giant cloud. The whole, created by bringing together individual units, forms something different and actually offers the opportunity to use many features together in different ways. The 'Transformers' movie is also the main theme of the swarm idea. You can create something different by connecting a few things together and use many features together. You reach something superior, higher quality, and more effective.

Many technologies we use in daily life have turned us into sensors and data sources. We all generate data. This data can be used in Russia, it can be used for intelligence gathering, and it can be used in war. Civilian use is now a very important part of the development of military technologies.



War is becoming increasingly complex, characterized by a growing number of new dual-use technologies, new actors, and new ways of waging war. It is difficult to predict how technologies will be used and misused in unintended ways.

Notwithstanding technological advancements, conventional weaponry and established combat methodologies persist as pivotal factors in determining victory. The caliber and volume of both personnel and armaments remain of paramount importance; industrial-scale warfare is not a relic of the past, but rather a continuing prospect of the future.



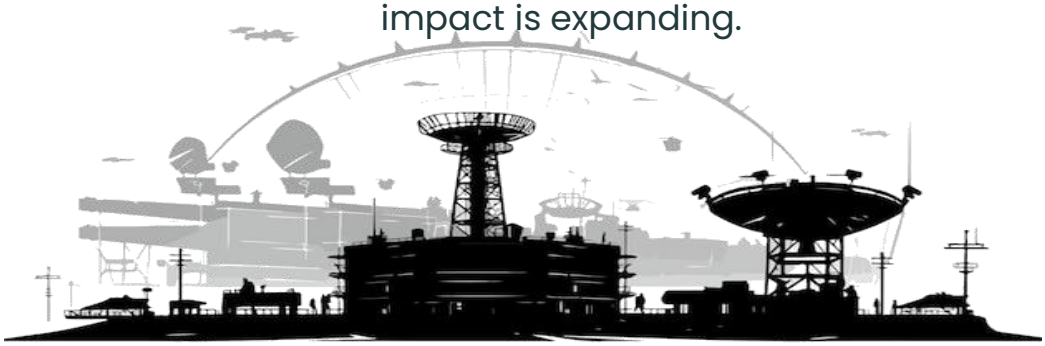
Future air power and combat systems will continue to evolve, predicated on cutting-edge technologies. The integration of these technologies into military systems underscores the critical importance of fundamental sciences, particularly mathematics, physics, chemistry, and biology, and the necessity of robust collaboration between these disciplines and the military sector—a matter of paramount national security. Proactive preparedness necessitates anticipating the realities your military will confront in the future. A technical solution can confer significant dynamism, though protracted discussions on adaptation and response may ensue. It is crucial to recognize that a prior technological innovation may inadvertently provide an advantage to adversaries.

In the future combat environment, artificial intelligence-supported analysis and decision systems will enable instant and accurate decision-making, while autonomous systems will minimize the human factor, reducing risks and increasing efficiency.

In addition to technological advancement, ethical responsibility and sustainability are other factors that will form the cornerstones of the military structure of the future. Weapon systems should develop sustainable environment and environmentally friendly solutions by considering the environmental impacts of military operations.

Moreover, the establishment of ethical and legal frameworks governing the deployment of artificial intelligence in combat scenarios is paramount for the preservation of human rights. Actions in this domain must be pursued with a proactive stance and comprehensive understanding. Global threats and security challenges transcend the capacity of any single nation to address. Consequently, international collaboration, the exchange of information and technology, joint training and exercises to ensure interoperability, and the consolidation of forces are indispensable for safeguarding collective security and peace.

With advancing technology, the variety and impact of threats on the battlefield are increasing day by day. Therefore, the tasks performed by soldiers are increasing, and the area of impact is expanding.

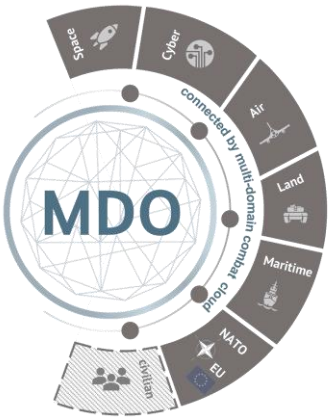


Should an attacker's tactical superiority ascend to a strategic level, the implication is that the system favors offensive maneuvers over defensive postures. In the delicate equilibrium between offense and defence, swarm technologies are poised to be a transformative element, reshaping combat doctrines and outcomes. How will you respond if you lack a system capable of neutralizing or engaging a swarm?

Future Soldiers must have the knowledge and skills to adapt to advanced technology and also develop ethical and leadership qualities. In this regard, the renewal of our education system and the continuous self-improvement of our military personnel are of vital importance. Because no matter how advanced the soldier's weapons and equipment are, the decision-maker in the future operational environment will still be a human. Considering this fact, it is an indispensable necessity that future soldiers are very well trained in technology and cybersecurity, hybrid operations, unmanned air land sea vehicles and autonomous systems, simulation and virtual reality, intelligence and analytical skills, psychological resilience, fast and accurate decision-making, competence and human management.

The concept of moving in swarms must begin with the fact that the swarm follows the behavior of the general leader of the swarm.

In a war environment where you have many different war vehicles and technologies, what you can achieve the most differently will bring success. Having access to these tools allows you to do a lot, but this does not mean that you know how to use them most efficiently, timely, or originally. So you have to make everything controllable for your structure and make it able to do the best. This will be most important whether you are the Pentagon or a drug cartel. The struggle for productivity, originality, having good human resources and being able to do the best will be the most important struggle in new war technologies as well.



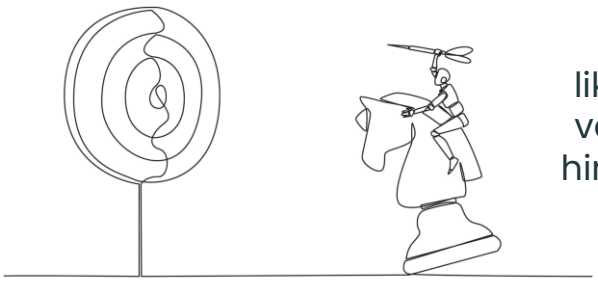
It is certain that future soldiers will be equipped with the opportunities offered by technology, and that the definitive result in battles will be obtained with the trained human factor in the future, as it has been in the past and present.

Technology is only as useful as its successful integration into tactics and doctrine. A technological advantage lasts only as long as the enemy does not adapt.

The battles of tomorrow will embody a confluence of both established and novel challenges, drawn from the annals of traditional and contemporary warfare.

Developing solutions that precisely align with your anticipated outcomes is of paramount importance. In asymmetric combat scenarios, the formulation of asymmetric response strategies is imperative.

Genetic modifications and biotechnologies, human body development programs, programs focused on protecting, collating, and activating the military more, and preparations for this should be made. These technologies are especially trying to make the military more ready in close combat and urban warfare environments.



Artificial intelligence can be likened to a toolbox, replete with various methodologies. Success hinges on discerning the optimal method to employ in pursuit of your strategic objectives.

The United States is working on autonomous swarm capability in a possible conflict between Taiwan and China. In other words, the big player is working on it. We will most likely have to be ready for this as well; it is very likely that we will encounter this problem in the future battlefield.

Genetic and cognitive augmentation is rapidly gaining prominence. Research is underway to enhance human physical and cognitive capacities, as well as situational awareness, through genetic modifications and augmentation technologies. Biotechnology is also increasingly favored for the purpose of elevating operational effectiveness.

Every technological development becomes a part of daily life after its maturation period and integrates with humans in a life-penetrating way. This can be called penetration, not innovation. Because it also reshapes the human.

Artificial intelligence-supported identification technologies blur the lines between war and personal security by increasing operational efficiency while shortening the time between intelligence gathering and technical deployment.

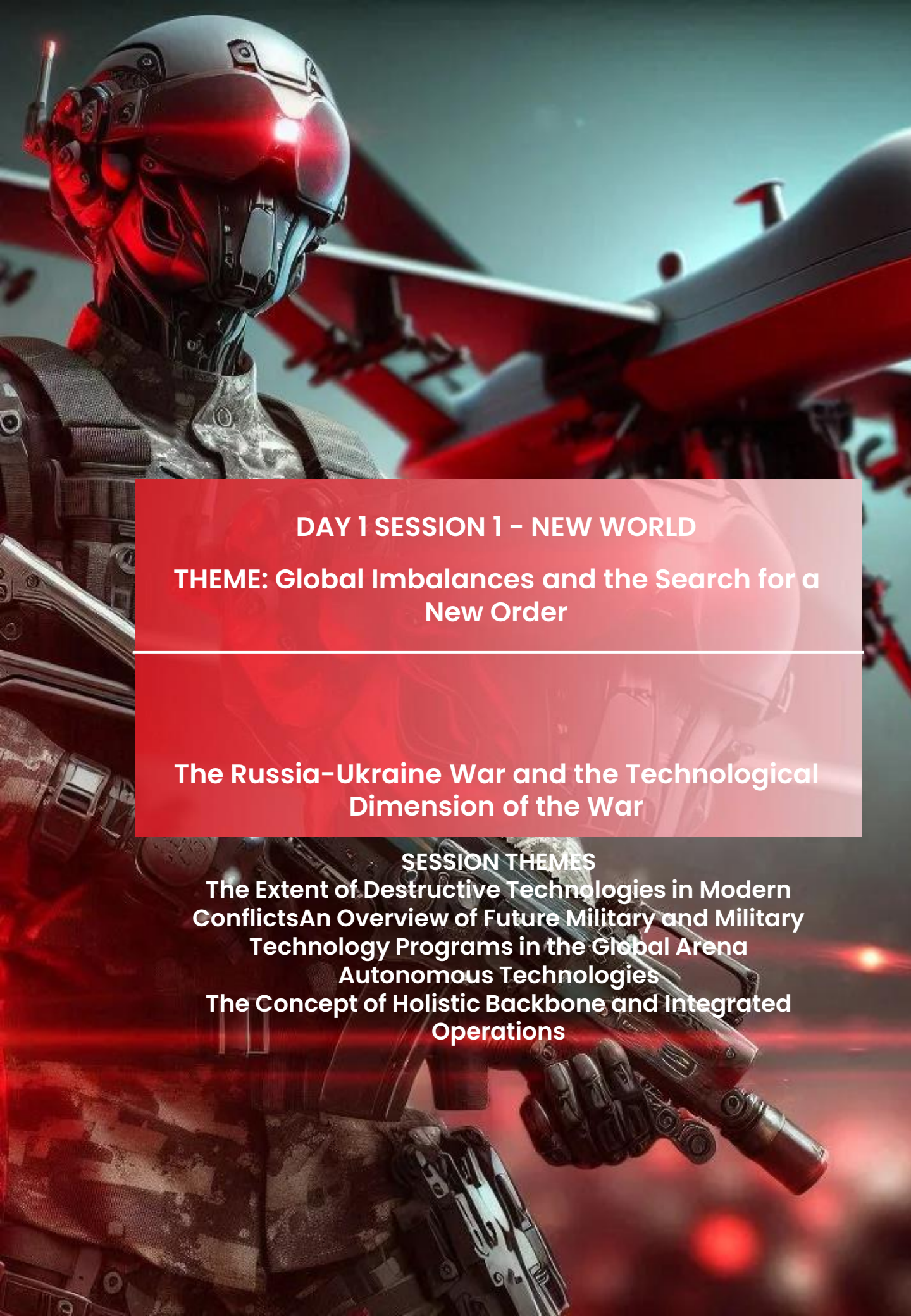
A shared and reliable working network is a necessity in the development of national military technologies such as artificial intelligence or autonomous systems. For example, soldiers are in favor of data protection, but engineers need data for development processes. Security or ease of work? A common working pool with layered, encrypted security systems is a must!

AI ARMY

DeepMind is actively developing cutting-edge technologies within the realm of deep robotics. Consequently, we anticipate witnessing the escalating influence of robotic and unmanned systems, particularly in coordinated swarm formations.

Many EU and NATO countries forget that we cannot create a common operational picture in artificial intelligence due to confidentiality. You cannot share data between different services, units, or countries.

The concept of a swarm entails overwhelming the adversary's defences. For instance, while Israel possesses a highly effective Air defence System, saturating it with a swarm would enable a portion of the attacking force to bypass its coverage, thereby achieving the swarm's objective.



DAY 1 SESSION 1 - NEW WORLD

THEME: Global Imbalances and the Search for a New Order

The Russia-Ukraine War and the Technological Dimension of the War

SESSION THEMES

The Extent of Destructive Technologies in Modern ConflictsAn Overview of Future Military and Military Technology Programs in the Global Arena
Autonomous Technologies
The Concept of Holistic Backbone and Integrated Operations

FIRST SESSION SUMMARY

Artificial intelligence is developing rapidly and is still in its early stages, much like the internet was when it first entered our lives. Countries around the world are working on the use of artificial intelligence in military systems. Numerous countries are competing globally in the field of lethal autonomous systems that can perform human-related tasks at cognitive levels. There is a risk that small states will lag behind in the face of systems using artificial intelligence and countermeasures. This could play an important role in changing global balances. In particular, a power struggle and technology war will take place in the effects of artificial intelligence on the seizure of systems, especially in electronic warfare and control systems. Especially after the development of Large Language Models (LLM) and in times when machines talk to each other, the decisions that autonomous systems will make cause concern, but they will be decisive, especially in conflicts. It is recommended that organizations such as NATO and the European Union closely follow developments and cooperate in technology development in line with the goals of China, Russia and the USA in this field.

It is important to develop the clothing and equipment of soldiers in close combat, especially against chemical, biological, radiological, and nuclear threats (CBRN) that can be used in unmanned systems. Additionally, such attacks that can be carried out with autonomous and robotic systems are among the newly emerging risk factors. The technologies used in today's conflicts provide ideas about the future war environments, and it is predicted that conflicts will move into the field of satellite and artificial intelligence-supported command and control systems.

The speed of taking precautions against developing technologies is also seen among the important messages brought by today's conflicts. Significant developments are also taking place in terms of war doctrines during the adaptation period between old and new technologies. The transformation of war tactics with the development of swarm systems is inevitable.

Artificial intelligence increasingly shows its effect as a force multiplier in the war environment.

Ukraine and Gaza are seen as testing grounds for conventional warfare, cyber warfare, smart robotic systems, and unmanned systems.

In the short term, the deployment of large robots in war environments will accelerate. In the medium and long term, it is predicted that wars will transform through cognitive warfare, which fuels autonomous and robotic conflicts, using methods such as social media, augmented reality, virtual reality, and efforts to read thoughts.

Erol YÜCEL PhD
HAVELSAN
MODERATOR

Distinguished guests, welcome to our "Future Soldier" organization. The theme of our first panel session is "Global Imbalances and the Search for a New Order." In this panel, our esteemed experts will share with us their insights on "The Extent of Destructive Technologies in Modern Conflicts, An Overview of Future Soldiers and Military Technology Programs in the Global Arena, Autonomous Technologies and the Holistic Backbone, Integrated Operation Concept." And they will share their findings on the technological dimension of the Russia-Ukraine War.

Mattias EKEN PhD
RAND
UK

Thank you for inviting me. I would like to thank the Turkish Ministry of National Defence and SASAD. This is my first visit to Turkiye, and I was told that my last name is actually a Turkish surname. And I have to make a small confession. Until a few years ago, I didn't know this. I am very happy that it is a country where my last name is not seen as strange. Thank you for welcoming me, I feel like I belong here.I would like to provide a kind of overview of the strategic implications of artificial intelligence, the risks and opportunities, and I think where we can go. Artificial intelligence is progressing at a rapid pace, with comprehensive consequences across society, the economy, and government as a whole. Turkey and other NATO countries have a strong artificial intelligence industry and academic research base and are important players. However, other countries are also investing heavily in this field and threatening to overtake them. This means that NATO allies have the opportunity to take advantage of and consolidate the early advantage of artificial intelligence. While artificial intelligence has great potential benefits, there are growing concerns around security bias and the consequences that may arise from disruption are being discussed.

There is a lot of exaggerated disagreement and uncertainty about the risks and opportunities of the increasing adaptation of artificial intelligence by militaries worldwide.

I think these discussions on artificial intelligence have second and third-order effects at the strategic level.

Artificial intelligence cannot and does not exist in a vacuum. In my opinion, there are more opportunities than risks. It is best to understand artificial intelligence as a complex, adaptable institutional technical system with a significant human component. It is important not to get too caught up in the technology itself due to various obstacles. Because various obstacles and facilitators will shape how quickly and in what way new artificial intelligence technologies will be incorporated into defence organizations.

We know that all kinds of technology are important in defence and their usage is widespread. Artificial intelligence is a member of the dual-use general-purpose technologies family, such as the engine, electricity, and the internet. Artificial intelligence technologies are software-based but, unlike traditional military technologies, they are also hardware-supported, hardware-enabled, which makes them quite elevated. Rapidly spreading artificial intelligence is there for much more than just a technology; for example, like a large language model such as Chat GPT for conversational purposes. Furthermore, innovation is driven by the private sector for commercial uses, not by the government or defence. The applications and consequences of artificial intelligence in the military field need to be understood collectively. The application areas and effects of artificial intelligence are evolving, but starting from a very low base, much of the discussion revolves around high-profile issues, this is prioritized. Such as Full Artificial Intelligence or Artificial General Intelligence (AGI), which can perform tasks at human-related cognitive levels, lethal autonomous weapons such as lethal autonomy. Unlike other issues, the discussion focuses on immediate consequences instead of the second or third-order consequences and effects of artificial intelligence that may be effective in the long term, instead of tactical, strategic risks or opportunities. General-purpose technology has the potential to significantly affect productivity in many sectors, including defence.

It is also dramatically transforming social structures and individual lifestyles. Artificial intelligence allows machines to

independently perform tasks that normally require human or biological intelligence, especially when the machine learns from data and learns how to perform these tasks independently. In this sense, AI has numerous potential impacts in all areas of defence, such as intelligence analysis, decision support tools, war games, simulation, electronic warfare, optimization of logistics, and so on.

It is also dramatically transforming social structures and individual lifestyles. Artificial intelligence allows machines to independently perform tasks that normally require human or biological intelligence, especially when the machine learns from data and learns how to perform these tasks independently. In this sense, AI has numerous potential impacts in all areas of defence, such as intelligence analysis, decision support tools, war games, simulation, electronic warfare, optimization of logistics, and so on. As a result, AI will transform the orchestration of strategy formulation, orchestration and completion, it will transform the productivity of the defence enterprise. It will also affect all the concepts we call the lines of defence, the efficiency and application of the entire force. It will affect military capabilities, readiness and Operational Deflection Patterns (ODS).

I will go into a little more detail about the impact of Artificial Intelligence Development (AI-D). The result I want to emphasize in particular is that artificial intelligence and the advantage will go to those who adapt best. In addition, the proliferation of military artificial intelligence and artificial intelligence in general will affect different international actors differently. At the strategic level, competition over military artificial intelligence can destabilize the super competition between the US and China and threaten other nations if new mechanisms are not introduced. Middle powers like the UK face difficult choices about how to focus the base's resources on how to shape asymmetric power and spheres of influence.

The global governance of military AI risks small states being left behind by larger players, but if some prove to be more agile in adopting military AI as it is, they can have an extraordinary impact at the strategic level. This is reflected in the foreign power of some countries such as Singapore, Finland and the Netherlands. There is an important distinction and line

between those who use AI ethically and those who do so with fewer restrictions. I think democracies have an advantage in attracting AI talent and nurturing innovation, but AI gives countries like China and Russia new tools to consolidate and export authoritarianism.

And what we are already seeing is that hostile forces are trying to export capabilities such as artificial intelligence and intelligent systems. With the use of Intelligent Systems in the military, we see them being deployed in countries around the world to finalize influence. With the development of these systems in the military also comes new risks and opportunities for different types of non-state actors, such as the private sector, but at the same time the situation is becoming more complex. The sovereignty of AI is about ensuring freedom of action and the legitimacy of AI governance. The legitimacy of artificial intelligence may allow extremist organizations or proxy actors to use artificial intelligence tools, for example, in areas such as recruiting militants, or in the financial planning and execution of increasingly complex attacks, including Joint Combined Chemical, Biological, Radiological and Nuclear (CBRN) and terrorist acts. As we have seen before, attackers, as seen in the Red Sea, proxy actors are already using smart robotic systems extensively.

With artificial intelligence, serious and organized crime groups can similarly gain increasing power, further intensifying this trend. Artificial intelligence can create new threats to international security, non-state actors, and acquire more complex artificial intelligence capabilities. Although a non-governmental organization (NGO) using artificial intelligence may not pose a direct military threat to Turkey or other NATO allies, they can still take action and lead to undesirable consequences if not handled carefully. Artificial intelligence can have profound effects not only on the military task forces and military capabilities that defence must provide but also on office functions that are generally overlooked in some cases. It can change the productivity, efficiency, and flexibility of defence Ministries and forces, the value for money of expenditures. Or we can quickly see them being left behind by more agile and innovative competitors. It can affect the effects on military and strategic competition. It is also used to affect how military capabilities are used. And it can also affect how

these effects can be seen in all parts that make up the whole. Artificial intelligence will be effective in every field from production to education. We will see a transition from linear development to spiral development and focus on software-centered models while providing platforms.

Our platforms will be geared towards leveraging human-machine teams and infrastructure power. The ideas at the heart of NATO's thinking on how to turn advantage into advantage are built on the maneuver approach. The task command within NATO decides on a course of action to outthink the enemy by observing their action repetition and analyzing their action cycle, to defeat them with an action cycle, and then to put the enemy into multiple dilemmas, working to shape their behavior in a way that supports NATO interests.

It is also important to note that if Russian and Chinese doctrines are framed through the lens of their own cultures and historical experiences, they also emphasize similar concepts. The Russian Armed Forces also emphasize making concepts such as the use of artificial intelligence and control reflexes functional and operational. Affecting the enemy's perceptions, access to the information domain and thinking, as well as disorder, trying to disrupt artificial intelligence-based systems, especially paralyzing enemy command and control structures in the initial period of war, is desired. Especially China is rapidly modernizing in preparation for war, which it calls system destruction, destruction of systems. The advantage with artificial intelligence comes not from destroying the enemy's forces in detail, but from targeting their key points and connections, targeting and weakening or destroying the power in their command. Confusion in artificial intelligence is used to confuse, paralyze and ultimately defeat command and control systems. And 'Informed or Intelligent Dimension Warfare' may be one of the terms in the literature. The meaning of this competition is a competition for advantage between opposing artificial intelligence-supported systems. Capabilities in the field of command, control, communications, computers, intelligence, surveillance, reconnaissance, target acquisition, commonly known as command, control, communications, computers, intelligence systems (C4I), such as military communications, calls, command and control, communications computers, intelligence, surveillance,

reconnaissance, target acquisition, etc., become both an advantage and a target. It can also be used as a defensive aid, such as poisoning training data for each side's adversary's AI algorithm, or as an AI support to exploit the limitations of AI systems.

For example, in addition to supporting automated cyber defences, artificial intelligence can also be used as a tool or defence aid to support attacks with a method such as mixing kinetic or non-kinetic effects.

In electronic warfare, it can also be used for purposes such as analyzing and targeting covert enemy communication and computer systems. Mobile centers can be attacked with long-range fire, and here the speed of artificial intelligence integration may be needed in target detection. Incorporating artificial intelligence into strategic decision-making processes to consider potential threat vectors where the enemy may misuse or disrupt the artificial intelligence system also means having technical and procedural redundancies and backward revisions.

If AI systems fail, the continuity of being able to fall back on systems that are not dependent on AI would also be an advantage in the event that an adversary abuses or disrupts the AI system. This is a case in point for the resilience and emergency preparedness of militaries around the world. For example, we are facing increasing demands to conduct humanitarian aid and disaster response operations, such as humanitarian crises, disaster response operations. AI can also help us by improving early warning systems for issues such as climate change and natural disasters, planning crisis response and resource allocation, and ensuring that critical assets are deployed and utilized when they are most needed. It can also be used as a way for civilian organizations to reduce the pressure on defence. AI is used for other military tasks, such as contributing to NATO operations, but it also generates new things.

And it can also create dependencies or resilience risks. For example, cyber attacks can weaken artificial intelligence systems. Artificial intelligence systems can lead to a lack of public trust with effectiveness, algorithmic, errors, effects, and

biases. Military artificial intelligence can be weaponized by enemy states or non-state actors to launch attacks on critical national infrastructure. It can be weaponized to attack supply chains or civilians.

The military use of artificial intelligence offers potential benefits in areas related to traditional nuclear and conventional deterrence, providing advanced analysis. However, it also brings risks and new uncertainties, such as the accidental targeting of nuclear command and control systems by artificial intelligence. Accidental targeting of these can escalate tensions. In traditional warfare, military artificial intelligence-supported military capabilities can increase speed, location, and lethality. In addition, it can also perform assistance-oriented data analysis without the need to expose human personnel to danger. It can help military commanders develop a more accurate and comprehensive understanding of the battlefield and enable them to be more informed. They can make informed decisions on how to deploy their forces, and with artificial intelligence, they can succeed in targeting long-range positions. It can improve the targeting of long-range position fires supported by the use of autonomous systems to help suppress enemy lines and missile defences.

We have seen that this technology has proven its value in various fields, including battle damage assessment, the intelligence community and information warfare, cyber warfare, logistics support and supply. Especially in the Ukraine and Russia war, remotely controlled autonomous systems were deployed and used in large numbers with increasing artificial intelligence and autonomy features. Ukraine even established a new military branch and unit on autonomous robotics and artificial intelligence systems. However, given the current situation, I think it is still clearly uncertain how such tactical effects will affect strategic outcomes.

Artificial intelligence can also help in peace building, tension reduction, conflict resolution and subsequent establishment of security conditions, security stability, and provision of welfare and security conditions. For example, it can help monitor and complete online hate speech, propaganda, or changes in public sentiment that could undermine any peace talks or fragile ceasefire in a conflict-affected area in real time.

Artificial intelligence, along with autonomous systems, can similarly be used in peacekeeping, peace enforcement operations, as well as mine clearance, disarmament of armed groups, and the reconstruction and implementation of destroyed and damaged infrastructure and services.

What are the most urgent threats related to Artificial Intelligence?

Our research covers several specific issues, including deepfakes, information and manipulation, political, economic, and social disruption, and artificial intelligence manipulations that distort the military decision-making process. Secondly, the empowerment of non-state actors with asymmetric capabilities to challenge NATO armies. There are also studies on biological and chemical weapons, but the current generation of large language models does not seem to have the ability to close the gap in this area. However, this should not mean complacency. We do not know, we cannot know, what Large Language Models (LLM) will do in the future. We must act by considering which area the ability to understand and produce will cover in the future.

Thirdly, the interlink effects of artificial intelligence. The struggle over the offense-defence balance in conventional warfare, tension dynamics, the instability of nuclear deterrence, especially in the concept of the intensification of superpower rivalries in a multipolar world already grappling with other factors of insecurity, to grapple with other drivers of insecurity in the long term and to distort the debate, and not to want to focus on the debate related to the future potential emergence of artificial intelligence.

Of course, I think there are security risks associated with artificial intelligence. Turkish defence can use artificial intelligence to prioritize policy interventions to reduce risks and maximize strategic interests. There are various methods that can be used to prioritize interventions to maximize strategic opportunities associated with artificial intelligence: In general, opportunities associated with artificial intelligence can be broadly grouped using risk-based methods. Is there a high level of confidence in projections for both the probability and impact of specific artificial intelligence-related trends? The first method is to focus on the best case against specific scenarios. The second is the uncertainty-based method.

Confidence in probability and impact predictions leads to a focus on minimizing regret across the widest possible range of scenarios. It is sound decision-making. The aim of conducting more detailed risk analysis can at most carry initial promises. The desire to engage in more detailed risk modeling, with an understanding of what artificial intelligence can do at a

technical level and how it is used in the real world, can be fed by various other analytical activities.

Allied adaptation to artificial intelligence will also create great opportunities, and building a local ecosystem for military artificial intelligence, making arrangements to create an ecosystem that shapes global spirit governance regulations will maximize advantage opportunities. This includes working with competitors to reduce tension risks. The main effort going forward should include a toolset consisting of efforts to increase the adoption of artificial intelligence. . It should also include efforts to limit its adoption by non-state and terrorist actors or hostile rogue states, and at the same time maximize its benefits to defence efforts to impose artificial intelligence. This struggle also incurs costs.

In the development process of artificial intelligence, an integrated and holistic approach is needed among NATO allies. In this field, like space, nuclear, biological and chemical weapons, to create a common industry and academia, civil society. However, artificial intelligence also has distinctive features that require a special approach compared to general-purpose technologies. A combination is needed to help shape the behavior of military artificial intelligence from a position of relative power. In order to ensure a clearer understanding of the strengths and limitations of military artificial intelligence, a clearer understanding of the perceptions, goals and limitations of different adversaries, measures to limit or prevent the increase of costs to competitors, intellectual property, data computation, infrastructure, deterrence, coercion, persuasion and shaping, such as new initiatives launched to develop the mapping of global artificial intelligence within the scope of a number of measures. There are more than 50 active regulations, some focusing on exploratory dialogue, some on voluntary principles and scope definition. Others are trying to develop more ambitious proposals for new regulations or policy guidelines. Like the UN Secretary-General's AI High-Level Advisory Board, the EU AI Act. Therefore, Turkey and NATO allies

should develop a proactive strategy to shape the artificial intelligence governance architecture. Like in nuclear deterrence, trust and momentum must be built towards the final consolidation of a solid structure.

Thank you for listening.

NOTES FROM THE PRESENTATION:

- With the widespread use of artificial intelligence, military artificial intelligence will affect the 'defence Development Line', which affects military capability and preparedness, including strategy development, regulation, and implementation areas of defence. The advantage will go to those who adapt best.

- I don't have a definite answer on whether and how different asymmetric power can compensate for this situation. However, China is focusing on this more than we are to compensate for some of its limitations and concerns, and I think we, as NATO and the West, need to find a way to counter this. At the same time, it may be necessary to do something to gain another asymmetric advantage.

Ridvan Bari URCOSTA
(PhD) UNIVERSITY OF WARSAW
POLAND

Hello, I am very happy and honored to be among you. It is a good tradition to introduce Turkish origins. I am a Crimean Turk, but I have been living in Poland for 10 years. I work on geopolitical futures and the main purpose of my work is to analyze exactly what is happening in the Russia-Ukraine War. I work on geopolitical futures. The main puprpose of my work is to analyze exactly what is happening in the Russia-Ukraine war. The global governance of military AI puts small states at risk of being left behind by larger players. Today I will go directly to war with basic specific concepts. We all remember the book Starship Troopers written by Robert A. Heinlein in 1959, it was also made into a movie. New versions were also written in 1999. In the book, while describing military life and the soldier of the future, for example, the clothes worn were called 'powerful suit'. What I saw in the war in Ukraine and the losses due to drones was this; FPV drones are really very different and deadly. What was mentioned in 1959 is the reality of today and painfully showed us that new clothes should be prepared for soldiers, especially precautions should be taken against these cheap killing tools made in China and the like. They are quite dangerous for both Russians and Russians. Look what the book says; «Our clothes give us better eyes, better ears and stronger backs. Strong legs to carry more weapons and ammunition. More firepower, more durability, less fragility». In fact, we can say that it is talking about the soldier of the future and artificial intelligence here, these references give us clues about artificial intelligence. Almost 70 years ago this topic was written. It was stated that additional placements to be made to the human body for the Future Soldier, even a kind of machine learning, should be integrated and these would have a serious impact on the soldier's combat capabilities. However, on the other hand, we must take into account that nothing has changed. When we examine the additional elements of the soldier's self-defence from history, exoskeletons are evolving, protective equipment is developing, and we should not ignore the future of the futuristic soldier we define as a space warrior.

History shows us this at the point reached. Perhaps if we look at what Elon Musk or the Chinese defence Industry are doing today, where they are today, we can think that this could be a reality by the end of the decade.

In summary, we don't know where we are approaching, so we can explain it theoretically. The scientific revolution we are witnessing can be explained by the Neolithic Revolution or can be based on Ray Kurzwell's assumption in his book 'The Singularity Is Near' that humans have surpassed biology. And this singularity should be at the end of this decade, that is, in the 2030s. Or the Industry 4.0 revolution. Concepts such as social utopia, anti-utopia, cyber, high technology-low life (cyberpunk) mentioned in the Neolithic revolution or artificial intelligence, space technologies, robotic technologies in the Industry 4.0 revolution, and eschatology dealing with the concept of 'end' and the evolution of non-biological systems entered our lives 100 years, 70 years ago and are starting to become our routine today. They are becoming a part of our daily lives and are pervasively integrating with us. The right word to describe this may not even be innovation, but penetration, which is defined as a virus entering a cell or an unauthorized attempt to access an information system or network. Because they are reshaping us. These are very serious events and we see that yesterday's past is today's realistic. We still don't know what Industry 4.0 will change and what it means, even Kurzwell could not fully explain while making assumptions. In summary, while a new society is being built, the shape of wars is also being rebuilt.

In addition to the Ukraine-Russia War, I would like to give an example from the war in Karabakh while describing the technological transformation of war; especially here, we are witnessing Turkey in the latest examples of technology. We can say that the monopolist, the leader of technology, has been in the West for the last few hundred years. The Soviet Union challenged technology in the 20th century, but this would not be entirely correct because the Soviet Union was also a part of the West in a way. We are currently seeing changes in this area since the beginning of the Karabakh War. Because since the Karabakh War, we see that some monopoly powers, leading powers have left the monopolization list, have separated from the traditional Powers list. In general, technological powers

produce unique things and dominate the new geo-economic and geopolitical structure, they offer it to the world market.

They do this with their own production chains, technology chains. This is a unique thing and can change the direction of countries, of us. This is generally a global dynamic, but at this point, there is a very special moment that we need to consider. I call these 'spark or sparks'.

Like Turkiye building its own independent military industry. Yes, but how long will this spark last, how long will the sparks last and turn into fire? Will it be able to create its own cycle in the future, will it be able to protect itself, will it be able to continue this spark and turn it into fire? It's good now, but can it go further? Will it be permanent in the future? All these findings also come from my analysis of the Ukraine War.

We all know that the concept of war is when we understand what your enemies are after. As Clausewitz said, 'War is a realm of uncertainty, three-quarters of the factors on which action in war is based are shrouded in a fog of more or less uncertainty.' The best examples are chess or real-time strategy (RTS) games. Although the area where you can make a move may not look like the battlefield in chess, you still cannot see the background in wars. You don't understand what your enemy is preparing, which means you don't understand what the enemy is. But you can see that unmanned aerial vehicles provide you with a top-down view at this point, you can reach some details, especially with those used in low orbit. Of course, there are obstacles with return, electronic warfare, signal jammers and similar technologies, but we can see that the strategies of the game, the rules of war are changing.

We can see that the Russians cleverly turned even the bad weather conditions in some parts of Ukraine (Kupyansk) into an advantage, using these systems in the field of intelligence, stabilizing the situation for themselves and complicating the situation on the battlefield. And with this, they were able to make a 5-7 kilometer advance. And here I can say that the connection of Artificial Intelligence and geospatial intelligence in the Low Earth Orbit (LEO) area was also used. They weakened or destroyed the defence lines. And in all of this, we can understand that the commander, just like a chess player, can

instantly control and change the strategy through virtual reality or instant data path, and change the game.

The space race, technological competition, resources and raw materials, industrial technology elites, strategy in the command and control room, integrated communication systems between all units (vertical and horizontal), the ability to create comprehensive geo-spatial intelligence, operational art, the redefined awareness dimension of situationality, tactics, information control and tactical units for the coordination of soldier's action are being reviewed, doctrines are changing, which constitute the war layers and space factor.

As the frictions, that is, the contacts on the battlefield change, the fog increases. Right at this point, something again shows a similarity to chess. You can see every move of your enemy, but you can be defeated or win, that is, you use your logic, Artificial Intelligence, drones and space technologies, but your brain is still the most valid weapon. So, even if the future war is different from previous wars, the strategy of commanders with serious intellectual abilities will determine the results. Those who know their capacities well and can use these capacities in the right place and at the right time will win. To win the Wars of the Future with the warriors of the future, you really need to be smart. Yes, Artificial Intelligence, Cloud Technologies, Autonomous Machines, Real-Time Strategy Simulations will be very useful, but you still have to be smart. The past tells us that those who command the war must be smart. Unmanned Aerial Vehicles, Bayraktar and the like give the feeling of the battlefield's vision and hearing.

Just like a Napoleon's desire to 'See the Entire Battlefield' in the past. Yes, technologies are reshaping old concepts. Space Technologies, Unmanned Aerial Vehicles and Artificial Intelligence intensify the revolution in tactical warfare philosophy and the concept of 'rear front'. It changes the technique, tactics, killing chain. The chain of find the enemy, suppress them with suppressive fire, surround the enemy, send the military close to the enemy and destroy all enemy fighters is changing tremendously. But in the Russia-Ukraine War, an example from the Assyrians living in the 2000s BC to the 21st century shows us the importance of using the mind.

The Russians used a weapon protection apparatus, which they called 'mangal' and which resembles a house in a triangular shape found in Assyrian reliefs, against FPV unmanned aerial vehicles.

If we look at how the Russians are advancing safely and protectively, and note that the Ukrainians are also using this method, we understand that they are using a simple but clever method for strong defence and fewer casualties. A strong defence for an expensive tank, but also a cheap method. And this should make us think in terms of making strong armored tanks in future wars due to unmanned aerial vehicles, or strong munitions on how to penetrate this. A tank not prepared for FPV drones in classic wars is quickly transforming in the battlefield with a simple mind, which is thought-provoking.

The war in Ukraine and Karabakh also gave some powers opportunities to enter the global market. For example, FPV drones quickly gained a market and grew rapidly as cheap and result-oriented products. If we return to the Russia-Ukraine War and proceed with concrete examples, we see that the Russians are on the field with the integration of several ideas, according to my observation and theory, the concept of Krank is a deep concept consisting of the combination of several ideas and they apply a kind of 'Strike Point Krank Concept'. Deep operation and war front, this has two meanings. One meaning is just a front, front line. The other meaning is that there are several armies on the front. For example, a specific unit or unit responsible for approximately 300 square kilometers. And this special unit has a kind of independence and autonomy in carrying out its own operations. Therefore, it implements its own decisions according to the conditions of the moment and applies the old Soviet Union concept in a modernized way as a deep operation in the regional area and on the front. And the Americans also admire this example in the network-centric battlefield.

By focusing on possible applications such as space intelligence with a denied access method, they carry out pinpoint strikes and record progress in a pinpoint manner. Advances in the Orikhiv, Kurakhov, Kurshchyna lines with methods such as drone intelligence and electronic warfare even reversed the comment s that Russia's two-star team

reserves would be exhausted. Especially throughout this process, we see that they have taken effective measures in supply and logistics, and that they have effectively used new technologies not only to kill, but also for sustainable warfare, and also in the supply force they have mobilized.

In addition, they can somehow direct the war as they want and succeed in drawing Ukrainian soldiers to the regions they want, and they make pinpoint strikes in the regions where they feel comfortable. War experts in Poland also agree on this. They advance by controlling a 30-kilometer line lengthwise and widthwise. If we talk about how Ukraine can respond to this advance, they use counter-artillery battery, electronic warfare, and unmanned aerial vehicles against this machine-like advance that creates a circular motion like 'Krank'. They even use fiber drones now.

Russia's stance against the advance is also related to the human resources, industrial capacities of the Ukrainians and the economic support of NATO countries, but the Russians are carrying out the advance by having the forces they have divided into regions advance in small areas, concentrating the forces in a certain area and doing this step by step. They are advancing step by step towards the West. And we must say that large smart bombs are also helping the Russians. And we must consider the effect of 'Battery' units, the smallest artillery unit in the army. The average range of Russian artillery is about 25-30 kilometers. Especially in the South, the Russian advances were due to the effect of these forces. They stopped every 10 kilometers of progress and prepared for another 10 kilometers. In other words, while the soldiers advanced and settled after the artillery fire, they prepared for the new 10-kilometer area. This was the answer to the question of why progress was not being made; 'Our Battery Units Must Be Ready for a New Assault.' And we see that they support the artillery fire with unmanned aerial vehicles, especially FPV drones. And again, the contributions of space technologies in the surveillance of the region. In other words, they are advancing to the front line with deep operations. And reaching the front line in total would be dangerous, it would also mean a lot for NATO countries. Ukrainians hope that they can use unmanned aerial vehicles as artillery. They have developed their own concept that unmanned aerial vehicles can replace artillery weapons in war,

stop or force the Russians for positional warfare. However, this did not work to stop the Russians.

Thank you, and with kind regards.

NOTES FROM THE PRESENTATION:

- Who controls the Moon, who controls the Earth's orbit, whoever controls the Earth's orbit, who controls the world's domains, and whoever controls these domains, including cyber, controls the world.

- The coming decades will be for control, presence, and deterrence competition for near-Earth orbit, the Moon, and Earth's orbit. It may be impossible to achieve great power status without being in orbit and on the Moon. And what about Mars, Mars is truly an astropolitical issue!

- Transparency has a geopolitical significance because those who control Earth's orbit and have key infrastructure there have full unrestricted access to the Earth's surface (the ability to monitor, surveil, project power, and detect changes and understand the impact).

QUESTION: I am a special operations officer. I want to see an enemy on the field, I want to see the performance of an extra skeleton or iron man on the field. For example, the importance of logistics in operations is very high, and in an environment where many electronic systems are used, a large number of battery shipments will be required on a high hill. For example, when an electronic system's battery runs out, I can be stronger than it. For example, what would the war be like if drones were not available in the Ukraine War? They spent 3,000 drones a day. We also use unmanned aerial vehicles against terrorist organizations and we are successful in this field. However, we see that the war still continues in logistics. I have attended many organizations on artificial intelligence and new technologies, everyone talks about high-tech weapons and optics, but I don't see anyone talking about logistics or energy. What is your opinion on this?

ANSWER: I am conveying to you a real war environment and my observations and findings. Logistics is the most important issue in war, I agree with you on this. But moving only through people with an approach that seems fantastic like Iron Man would be falling into a trap. You cannot stop while your opponent is developing new technologies. For example, I watched a very old video of Selçuk Bayraktar. In the 2000s, he was trying to explain his vision to someone and was defending his idea, which was not mainstream today. That day, he argued that the technology he had was a technology issue that would affect the future, that is, today. I agree with you, we must be cool-headed against philosophical thought, but we must not forget that realistic thoughts can shape the future one day, and we must be cool-headed about this as well. We must not forget that logistics will also be solved with developments.

Dr. Jean-Marc RICKLY
GCSP
İSVİÇRE

Thank you for your kind invitation. I will talk about what we witnessed in the war in Ukraine. We will examine the role of artificial intelligence. The main purpose of artificial intelligence and what it is really good at is breaking down data and analyzing it. Therefore, the greatest contribution we currently have and are witnessing is an analytical facilitator. However, we also see that artificial intelligence is increasingly being used as a force multiplier fire.

In the war environment, artificial intelligence is a force multiplier, analytical enabler, and destructive power. And I will try to explain what I mean by this and give some concrete examples. Ukraine, like Gaza right now, is an incredible test laboratory for the use and testing of these technologies.

And that's why here are a few examples. AI was; in fact, it was used to process data to improve all intelligence and regional images. You may have heard of the GIS Arta application, which basically mimics the Uber application but is used to connect the driver with the customer or passenger. They developed a similar application from September 2022, when the Russians started using Shadid 136 kamikaze drones and the Ukrainian air defence was suddenly overwhelmed. Any Ukrainian citizen can download this application and support the coordination of artillery attacks or drone intelligence. Any Ukrainian citizen can download this application and support the coordination of artillery attacks or drone intelligence. With this application, which has fast targeting and is used by Ukrainian artillery, you can simply point to the drone and the image will be localized, analyzed and included in the intelligence cycle, the intelligence cycle can be fed. What we need to know is that we need to realize that each of us has now become a sensor, we are generating data. This data can also be used in Russia and can also be used for intelligence purposes. Russia and Ukraine receive support from some start-up companies. For example, primer.ai primarily uses NLP in new language programming to analyze a similar question to Google's on text.

When you have a new technology, you have an interesting system that you can develop and create clear images, it's basically a job-collecting application, it's quite simple, they collected all the pictures and compared these pictures with other pictures and thus created a portable mini-intelligence agency. During that war, the Ukrainians used these images to determine whether Russian soldiers were dead or alive. And once you learn who they are, you can also know who their family is. And you can deliver your targeted messages.

So, the first force multiplier of artificial intelligence is clearly this, and it's not new, but Ukraine is a battlefield where many different technologies are used and it's very dynamic, we are witnessing this. At the beginning of the war, Ukraine's advantage against Russia was provided especially with Bayraktar TB2, but over time the Russians adapted, and what we see is a constant pace of innovation. Thanks to the private sector and new initiatives, there is a constant pace of innovation on the battlefield. For example, there were even companies that did not work in the defence industry. A company that basically used artificial intelligence to identify fruits on trees changed a few parameters in the algorithm to identify the target and the environment after the war started. In 2020, we witnessed the emergence of kamikaze drones in Karabakh, that is, unmanned aerial vehicles and the area are activated when they receive the signal later.

The Russians acquired and used Shahed 146s from Iran, contributing to the blackout of many regions of Ukraine by targeting electricity distribution between February and November 2022. So there was almost no light, and the Russians managed to turn off the lights in Ukraine. Whether on the Russian side or the Ukrainian side, you are weaving together the entire family of a large nation entering the battlefield. This clearly leads to countermeasures, especially electronic warfare, and the success rate of FPVs dropped dramatically due to jamming, and therefore both Russian and Ukrainian actors had to adapt to these developments. Both sides tried to exert pressure with their own capabilities, and this time counter-jamming systems came into play.

This clearly leads to countermeasures, especially electronic warfare, and the success rate of FPVs dropped

dramatically due to jamming, and therefore both Russian and Ukrainian actors had to adapt to these developments. Both sides tried to exert pressure with their own capabilities, and this time counter-jamming systems came into play.

The Ukraine-Russia conflict is likely one of the first examples of a major robot war, and it is one of the first robot wars in which a large Russian robot was destroyed by an unmanned aerial vehicle. And that's why we're no longer entering science fiction here, we're entering this kind of dynamic. It was reported that at the beginning of September, Ukrainians launched an attack with a robot against a Russian trench.

What we clearly and truly need to understand is that this technology is proliferating and democratizing very, very quickly. Okay, this is different from nuclear and doesn't resemble it, but once code lines are out, they are always out, and non-legal actors can really use them. For example, this was the case with ISIS in 2017, the drones used could be modified with small ports to carry grenades, and caused up to 30 Iraqi soldiers to lose their lives per week. This was the first time in the history of warfare that a non-state actor managed to gain a tactical advantage over state actors. You know, especially the flying AK-47s made with the kind of drones you can find on the market now. And cyberspace, you know there were a lot of cyber attacks during the war in Ukraine and it was a disappointing situation, cyber played a role even before the war.

Our role before the war and it also plays an important role in destruction. And in fact, cyberspace was actually used to silence targets before the war. If you remember the first day of the war, it was a cyber attack against the satellite, and the system disabled the satellite effect on Ukraine, Germany, and other countries. But what's interesting is that this satellite system was replaced by Starlink, and who is Elon Musk, a person you know, and what's interesting is that you also account for the power of a single individual in threat analysis and strategic analysis. Because now, according to the mask Trump wore when he was elected president, what Trump said was; "Hey Ukrainian, you should start talking to the Russians for peace and make a peace plan now.

This guy has his hand on the button, and this already happened in Crimea; Starlink essentially blinded the region. Ukraine couldn't use its capabilities.

As a strategist analyst, the title of my last book was 'Proxy War,' and in the book, I stated that future wars would be waged and gains would be achieved by states and intra-state actors using either human or technological proxies. The war in Ukraine showed that this is a very vivid claim and example.

Ukrainians are asking for help from abroad. Anyone who wants to join the Ukrainian Army can join, but as an operations chief or commander, you face a real problem. You have absolutely no control over your proxies, and it creates a liability issue.

Interestingly, autonomy is increasing in weapon systems, and we need to think about how to integrate this autonomy with humans, this growing autonomy. Let's look at it this way, I was trained as a fighter pilot in the air force, and my training cost about 1 million Swiss francs. And the US Army Air Force is conducting a test this year, tests where an algorithm can fly a jet autonomously, and this system can perform 8 different tasks. So now think about how you will integrate these kinds of capabilities in the future, and think about what to do because artificial intelligence works much faster than we do. We operate in half or 1 second, but artificial intelligence operates at nano speed. We really need to bring together ways to partner, we need to find a way to partner through human-machine.

Artificial intelligence can disrupt wars, something more and more can be done about it. For example, swarm technologies, most recently more than 10,000 drones were flying together in Shenzhen and that was a world record. Drones were starting to replace fireworks. Obviously it was very beautiful but in the military this has a very powerful impact. Because the idea of a swarm is to saturate your enemy system and for example the Israeli Air defence System is really good but if you saturate that system then some will break through and the swarm will succeed. We are starting to witness this. War is turning into this, the second effect, although less visible, shows that it is deeper.

For example, in a flock of birds, no bird is aware of the shape that is formed, like a giant cloud. If you put individual units together, you create something with different qualities, you can use many features together differently. For moviegoers, this is a swarm idea with Transformers, you connect something together and suddenly you make something new that is superior in terms of quality and impact.

Two years ago I had a meeting with Google's Deepmind team working on artificial intelligence and I was in a meeting with the head of the deep robotics department. They are doing studies on emerging technologies just like other companies working in this field. So we will see increasingly more swarms in wars in the future. And they can produce this faster, it increases with milk, so you saturate the enemy system and now you can do more damage. They had also used thermobaric bombs to target bunkers in Odessa, the target of these bombs, as you know, is to absorb oxygen and basically burst your lungs, your eyes also burst

A simulation conducted two years ago by the US Army indicates that we need to invest in capabilities that transform into a fully autonomous swarm in the event of a possible invasion of Taiwan by China. So the big player is working on this and it is very likely that we should be ready for this, we will encounter this problem on the battlefield in the future. The problem with swarms on the future battlefield is that it has a serious impact on what we call the offense-defence balance right now. We do not have a system that can affect, strike a swarm. So you may have a different system that can counter all swarms. Because we are a defence-dominant international system due to nuclear deterrence. My argument is that if this offensive tactical advantage passes to a strategic level, it means that the system is advantageous to the offense over the defence. In such a situation, what is the best way to protect yourself? Attacking first is a violation of Article 2.4 of the United Nations. The UN Charter calls this prevention, so potentially this technology has the potential to completely reverse the international UN charter.

The last way we can think of artificial intelligence as a disruptor is information and destruction, and information operation destruction is not new. It has been going on since the

Roman Empire and only the tools are completely different.

What has changed is the tools, and now they are scalable and measurable. Deepfakes were invented in 2014. You can deliver any message you want with one of two pictures or images. The images launched in 2018 are really very realistic. These were first used in the war in March 2022 and made Zelensky call on citizens to lay down their arms. We had also seen Ukraine's attempts of this kind as videos. We saw that the Russians again used thermobaric loads (vacuum bombs) together with Shahed 136 unmanned aerial vehicles. Last June, Putin's mass mobilization message, which resulted in the declaration of martial law, was published. And it caused panic scenes in some cities of Ukraine. Now, in 2013, as a military analyst, how would you ask how this information will be managed 10 years later?

You will have to find a technology that is not scientifically there, you will have to understand how it works in a war environment and understand how it can be used. This is exponential growth and it is also an exponential growth on the battlefield. Therefore, you really need to think outside the box. Because understanding the level that this technology provides is very important. For example, earlier this year, the Russians deepfaked a TV host from France 24, and basically the host announces in the video that French President Emmanuel Macron has postponed his trip to Ukraine because French secret services thwarted an assassination attempt against him. So what does this mean? Why is deepfaking so important? Because structurally we all have psychological biases and during these biases an asymmetry occurs. We tend to prefer lies over facts and lies travel faster. And the structural asymmetry of mankind is to reach a much wider audience.

Now we come to Cognitive Warfare. Cognitive Warfare is the sixth domain of war. Your brain actually becomes the battlefield first by locking you into an information environment, and it is more than just information to reconstruct what you perceive. Because Cognitive Warfare is the ability to control what and how you think, it is structured to control how you think.

As you know, war is becoming more cognitive. War is now locking into virtual environments, including metaverses and immersive technologies.

You may have seen the Apple Vision Pro earlier this year. You now have glasses that begin to track your brain activity. A specific object or person triggers a specific brain activity and you begin to track and correlate emotional responses such as where you are looking and what you are feeling. This opens the door to perfect manipulation. We saw in another version of a test we did by putting people in a Magnetic Resonance Imaging (MRI) device for a test in 2018 that we are now entering the age of mind reading. An era where Artificial Intelligence interprets what we see, hear and feel. Okay, the machine is increasing and will be able to read minds? What's the next step? The next step will be to rewrite your memory. We are not there yet, we are far from there, but you need to include this in your analysis.

What does this mean for us? I'm talking about emerging technologies here, but the losses we've seen in the Ukraine War are similar to the French losses in World War I. According to reports, a Russian soldier was dying on the battlefield every 44 seconds, but we are also witnessing new types of weapons entering the war. What I've shown you here doesn't seem to be big robots or technologies that will change the balance for now, but we need to be aware of the future of these things. And this creates new dynamics, it doesn't mean that the previous weapons and dynamics are gone, no, you have to take the new and the old into account together. You also have to take into account the fact that we need to integrate more and more people into innovations and integrate machines and humans. Obviously, the intelligence of machines raises a lot of ethical concerns. It also creates a lot of ethical concerns in terms of accountability for too many casualties or lives saved.

Thank you.

NOTES FROM THE PRESENTATION:

- The force multiplier, analytical enabler, and destructive effects of artificial intelligence are inevitable.
- War is becoming increasingly complex, characterized by a growing number of new dual-use technologies, new actors, and new ways of waging war. It is difficult to predict how technologies will be used and misused in unintended ways. Failure of imagination is always a valid risk.
- Even with the development of technology, traditional weapons and ways of warfare remain dominant and key determinants of success. The quality and quantity of personnel and weapons continue to be vital, industrial warfare is not behind us.

- "When you start stacking accelerations on top of each other, you will soon have autonomous drone swarms with facial recognition attacking you on the battlefield. So how will you stop that?"

QUESTION: What is your thought on the demand for traditional ammunition and the increase in ammunition factories despite all technological developments? Is the depletion of ammunition due to poor planning or the impact of new technologies used on the battlefield?

ANSWER: When we see a new technology entering the battlefield, it doesn't mean that the previous dynamics are gone. If you look at the situation in Ukraine, in terms of Europeans and the dynamics of 10 years ago, nobody would have believed if you had said there would be a major war similar to World War I in terms of losses. But what happened, you see trench warfare similar to World War I. For example, drones increase the transparency and visibility of the battlefield to a high level for the infantry soldier. Being an infantryman on the battlefield is really hard work. First, you create new ways for implementation, then you try to neutralize the enemy. And for this, you need ammunition. When you combine traditional methods with developing technologies, you create new dynamics. We are talking about the fog of war, friction. This is an evolving game, war has always evolved. In fact, we are currently talking about something where the path related to the brain can be directly changed.

DAY 1 SESSION 2 - NEW WAR

THEMES:
Modernism in Warfare: Technological Actors
SESSION SUBJECT:
Karabakh War: The Effects of Technology on War Doctrines

SESSION THEMES:

Air Power in the Modern World: Autonomous Systems and Wars

Robot Soldiers and a Perspective on War with New Technologies

The Intersection of Technology, Security, and Geopolitics

SECOND SESSION SUMMARY

The operational effectiveness of the Bayraktar TB2 in the Nagorno-Karabakh conflict, the advancements that contributed to Russia's initial setbacks during the early phase of the Ukraine War, and the ensuing countermeasures are all emblematic of the rapid and dynamic shifts inherent in next-generation technologies. A paradigm shift is underway, transitioning from a human-centric combat environment to a technology-dominated battlespace.

Blockchain technologies are of great importance for quantum computers and big data usage, as well as internet of things technologies. Especially for secure communication, decision-making and secure data sharing, it offers opportunities with its decentralized but data immutability structure. Companies such as DARPA, Lockheed Martin, and Boeing are working in this field in the world. Planning is required to prepare for the multiple different environments of the future. It is predicted that global proxy actors such as Elon Musk may increase in the future in areas such as artificial intelligence, neuralink, and space, and may become dangerous actors with new technologies. Neuro warfare and cognitive warfare can be seen as a military activity in the future. There will be a need for very different human resources in very different fields. It is necessary to prepare for uncertain environments and uncertain events, also known as Black Swan. This will make it mandatory to establish a good human resource and a dynamic structure.

Contemporary conflicts are increasingly viewed as proving grounds for the evolution of both traditional and cutting-edge military technologies, serving as arenas where innovation and feasibility are rigorously tested. A competitive landscape prevails, wherein human judgment alone is deemed insufficient, necessitating the mobilization of technological capabilities for swift and precise decision-making. 1 The prospect of artificial intelligence autonomously operating beyond human oversight presents a significant future concern, demanding readiness for the advent of 'ghost warfare.' Cyber warfare possesses the potential for a smaller nation to inflict substantial damage upon a significantly larger adversary. The race to identify and mitigate vulnerabilitie s in satellite and spectrum technologies

Lieutenant General (Retired) Alparslan ERDOĞAN
MODERATOR

Welcome, esteemed guests. The subject of the future soldier and the future battlefield has been a perennial topic of discussion. As a graduate of the Military Academy, I recall that throughout my time as a cadet, and later during staff training, we frequently deliberated on the characteristics of the future soldier and the evolving nature of post-combat scenarios. We have observed a shift towards technology, rather than solely focusing on the soldier.

We are currently witnessing a transition from a human-centric war arena to a technology-driven combat environment. Approximately three decades ago, I participated in a 'Future Soldier' conference hosted by the NATO Land Armaments Group. The conference's central focus revolved around the optimal design of ballistic protective helmets, vests, and small unit-level communication systems. In contrast, our current discussions center on artificial intelligence, human-machine interfaces, robotics, unmanned and autonomous systems, and digital command structures. This evolution highlights the significant progress we have made, transitioning from basic head and body protection to these advanced domains. Many militaries have begun establishing dedicated units for autonomous and unmanned systems. With our EDHOK commander present, I would like to advocate for the Turkish Armed Forces to consider similar restructuring, such as creating an Autonomous Systems or Unmanned Aerial Vehicle Command, either on a joint or service-specific basis.

Assos. Prof. Dr. Muharrem Tuncay GENÇOĞLU
FIRAT UNIVERSITY

Distinguished commanders, esteemed participants, I extend my warmest greetings to you all. I would like to express my deepest sympathies to the families of the martyrs who tragically lost their lives in the recent abhorrent attack and offer my sincere condolences to the TUSAŞ family. In my address, I intend to delve into a slightly divergent perspective.

I will address the security implications arising from the ongoing conflicts in our vicinity, specifically focusing on drone warfare and air power operations, due to the substantial communication and data streams generated during these engagements. My focus will be on this particular aspect, specifically exploring how blockchain technology can enhance the efficiency of autonomous systems within air forces, its implications for modern warfare, and the geopolitical ramifications of these advancements, illustrated with real-world examples. The contemporary battlefield is experiencing a transformative evolution driven by the integration of cutting-edge technologies. We have observed the escalating deployment of unmanned systems in our immediate region, notably in conflicts such as the Syrian Civil War, the Second Nagorno-Karabakh War, and the ongoing Russo-Ukrainian War, particularly in tactical and operational contexts. The Nagorno-Karabakh conflict, in particular, serves as a compelling case study, demonstrating the paradigm shift in modern warfare enabled by technology. Autonomous systems, unmanned aerial vehicles (UAVs), and robust digital infrastructures have decisively shaped the conflict's trajectory. Azerbaijan's adept utilization of unmanned combat aerial vehicles (UCAVs) and UAVs to target enemy defences and secure strategic advantages underscores the critical role of modern technologies in contemporary military operations. Consequently, the imperative for secure, effective, and coordinated autonomous systems is paramount. It is evident that this is a matter of utmost importance and urgency. Traditionally human-centric air power is undergoing a metamorphosis driven by autonomous systems, robotic

technologies, and, notably, blockchain technology. This transformation is fundamentally altering nations' perceptions of security, geopolitics, and technological dominance.

Autonomous systems, particularly technologies like unmanned aerial vehicles (UAVs) and drone swarms, have become integral to modern air power strategies. The Turkish-made Bayraktar TB2s, deployed in the Nagorno-Karabakh War, played a pivotal role in target identification and neutralization, thereby influencing the conflict's outcome. These systems offer the capability for rapid and precise strikes while minimizing human risk. However, their efficacy hinges on secure communication, decision-making, and data sharing. We are witnessing the emergence of a new paradigm in autonomous systems and air power, necessitating a re-evaluation of autonomous air power, with a keen awareness of both its challenges and opportunities. From this perspective, we can analyze the challenges related to data security, coordination, trust, and accountability. UAV communication systems are susceptible to enemy cyber attacks, exemplified by Russia's use of electronic warfare systems in Syria. Coordination of distributed air assets, such as drone swarms, requires seamless and decentralized control.

Furthermore, determining accountability in autonomous systems' decision-making processes remains a contentious issue. Blockchain technology emerges as a promising security and technological solution, potentially addressing these challenges and shaping the future of autonomous air power. Blockchain technology presents a significant solution to the security and coordination challenges inherent in autonomous air power systems. Its distributed, decentralized, immutable, and transparent architecture ensures secure communication, efficient coordination, and robust accountability. To briefly explain blockchain, it originated as a financial technology, introduced in 2008 through a seminal paper. While it is widely associated with cryptocurrencies like Bitcoin and Ethereum, it is essential to recognize that blockchain's roots extend to the 1980s, grounded in mathematical principles. Its core strengths lie in its distributed and decentralized nature, coupled with its transparency. The immutable characteristic of data recorded on the blockchain offers unparalleled security, particularly in data and communication domains.

As the name suggests, blockchain is a technology wherein each block possesses a distinct security and hash value, facilitating its linkage to the subsequent block. Once data is entered, it becomes immutable due to network-wide validation, thereby fostering trust through immutability and transparency. Such is the essence of blockchain technology.

The fundamental characteristics of blockchain technology include: its distributed architecture, ensuring that every data entry is replicated across thousands of nodes within the network; its inherent transparency, enabling the tracking of all transactions; and its immutability, which safeguards data integrity by preventing unauthorized modifications. These attributes position blockchain as a pivotal technology, poised to form the backbone of the next-generation internet. It is imperative that we seize this opportunity and remain at the forefront of this technological evolution.

In what domains is blockchain technology being implemented within military contexts? Applications include the storage and safeguarding of classified and critical data, ensuring the integrity, confidentiality, and veracity of communications, network-centric warfare, integrated air defence systems, and the enhancement of global supply chain efficacy. This technology finds its most prevalent use within supply chain management. We can also observe blockchain's utility in secure data transmission, decentralized command and control, supply chain governance, and its impact on accountability and ethical considerations. Furthermore, blockchain technology offers significant contributions to the fields of robotics and the future of warfare. As is well-known, autonomous weapon systems are revolutionizing warfare by minimizing human involvement. The synergy between blockchain and robotic technologies promises to augment the reliability and effectiveness of these systems.

For instance, autonomous robotic defence systems deployed along the South Korean border can achieve enhanced reliability through blockchain integration, a development we observe in their ongoing projects. Blockchain technology offers significant benefits in areas such as tamper-proof identity management, improved collaborative capabilities, and the deterrence of unauthorized actions.

Notably, China is pursuing a project focused on implementing blockchain-based identity management for military robots, particularly in the realm of manipulation-resistant identity.

As the name suggests, blockchain is a technology wherein each block possesses a distinct security and hash value, facilitating its linkage to the subsequent block. Once data is entered, it becomes immutable due to network-wide validation, thereby fostering trust through immutability and transparency. Such is the essence of blockchain technology.

The fundamental characteristics of blockchain technology include: its distributed architecture, ensuring that every data entry is replicated across thousands of nodes within the network; its inherent transparency, enabling the tracking of all transactions; and its immutability, which safeguards data integrity by preventing unauthorized modifications. These attributes position blockchain as a pivotal technology, poised to form the backbone of the next-generation internet. It is imperative that we seize this opportunity and remain at the forefront of this technological evolution.

In what domains is blockchain technology being implemented within military contexts? Applications include the storage and safeguarding of classified and critical data, ensuring the integrity, confidentiality, and veracity of communications, network-centric warfare, integrated air defence systems, and the enhancement of global supply chain efficacy. This technology finds its most prevalent use within supply chain management. We can also observe blockchain's utility in secure data transmission, decentralized command and control, supply chain governance, and its impact on accountability and ethical considerations. Furthermore, blockchain technology offers significant contributions to the fields of robotics and the future of warfare. As is well-known, autonomous weapon systems are revolutionizing warfare by minimizing human involvement. The synergy between blockchain and robotic technologies promises to augment the reliability and effectiveness of these systems. For instance, autonomous robotic defence systems deployed along the South Korean border can achieve enhanced reliability through blockchain integration, a development we observe in their ongoing projects. Blockchain technology offers significant

benefits in areas such as tamper-proof identity management, improved collaborative capabilities, and the deterrence of unauthorized actions. 1 Notably, China is pursuing a project focused on implementing blockchain-based identity management for military robots, particularly in the realm of manipulation-resistant identity systems.

It aims to prevent manipulated attacks with blockchain. Again, when we look at the point of cooperation, these autonomous systems can be managed securely with a common network.

Each robot or drone will be assigned a unique blockchain identity, guaranteeing operation solely within predefined parameters, thereby ensuring control exclusively by authorized personnel. China is developing blockchain-based identity management systems for its military robots. Autonomous systems can leverage a shared blockchain platform to rapidly exchange intelligence and collaboratively adapt their strategies in dynamic combat scenarios. The United States Air Force is currently conducting trials on real-time information sharing among autonomous drone swarms via blockchain technology. These systems are designed to enhance intra-swarm coordination, enabling more effective target engagement.

From a geopolitical and security perspective, blockchain has the potential to influence not only the battlefield but also global alliance dynamics. It is a critical technology capable of reshaping security doctrines and redefining geopolitical strategies by integrating air power with domains such as space, cyberspace, and land operations. This allows for the examination of geopolitical and security impacts, including technological arms races, coalition operations, and cybersecurity priorities. Blockchain's ability to integrate air power with other domains empowers it to redefine security doctrines and geopolitical strategies. Future applications may include smart contracts for rules of engagement, impacts on predictive analytics and artificial intelligence, and a visible influence on global governance.

In the realm of blockchain applications for air forces, the projects undertaken by the United States Air Force are

particularly noteworthy. The US Air Force, in collaboration with SIMBA Chain, is employing blockchain technology to enhance the traceability of aircraft components manufactured through 3D printing and to bolster supply chain security. This initiative seeks to mitigate the risk of counterfeit critical parts and to foster greater process transparency.

Under the Strategic Technology Focus Initiative (STRATFI), the United States Air Force has allocated $30 million to SIMBA Chain. This investment supports the development of blockchain-based solutions and the enhancement of supply chain management. These technologies are applicable not only to the Air Force but also to various other military branches and logistical operations.

The United States Air Force is transitioning from theoretical exploration to practical implementation of blockchain technology. Through the utilization of SIMBA Blocks, they are addressing critical requirements such as tracking fund disbursements and digitizing supply chain transactions in the Digital Blockchain Budgeting Accountability and Tracking (DiBaT) project. The US Air Force has also commenced efforts to develop a blockchain framework that prevents the infiltration of espionage chips into military hardware. Concurrently, DARPA is conducting blockchain trials to revolutionize battlefield operations management concerning efficiency, resilience, and security. Additionally, NATO is leveraging blockchain to ensure secure military supply chains and auditable logistics services. These are among the notable examples we are observing.

Additionally, blockchain technology will provide significant opportunities across four key areas: management of defence war operations, logistics and supply chain management, autonomous drone swarm control, and border security. For the Air Force, blockchain presents an advantage in securing avionic systems. As recently demonstrated by the United States with the flight of an AI-equipped F-16, safeguarding AI-driven defence systems using blockchain is a focus of DARPA's research. Integrating blockchain with AI-supported autonomous systems is crucial for enhancing security and traceability. We must ensure that blockchain technology is seamlessly integrated with artificial intelligence.

Unmanned aerial vehicles collect and analyze data in the battlefield. Blockchain technology must be used to securely store and record this data. With blockchain, this data can be encrypted in a decentralized structure and the security of operations can be increased.

NATO is incorporating blockchain technology to bolster the security of its cyber defence initiatives and AI-driven cyberattack detection systems. defence contractors, including Lockheed Martin and Boeing, are integrating AI and blockchain into their defence systems, particularly developing blockchain-based solutions for aircraft and air system maintenance and operations. The United States Air Force is actively exploring the potential of blockchain technology in aircraft maintenance management and logistical operations through various projects.

These projects aim to enhance operational efficiency by improving the traceability of aircraft component replacement and maintenance procedures. Looking ahead to the future of security and cyber defence, air forces will need to leverage both artificial intelligence and blockchain technologies to ensure robust security and defence against evolving cyber threats. The integration of these two technologies, particularly within the cybersecurity domain, will be pivotal in safeguarding the Air Force's digital infrastructure.

Artificial intelligence serves as a vital instrument for the detection and mitigation of cyber threats, while blockchain technology enhances cybersecurity by enabling the traceability and logging of these attacks, adding an extra layer of defence. AI-driven projects within the defence sector will enable air defence systems to autonomously analyze threats and implement defensive measures. By integrating domestically developed AI and blockchain solutions, these systems can achieve heightened security. We are actively pursuing these technologies and must continue to advance them. Prominent entities like Turkish Aerospace Industries Inc. (TAI) are engaged in projects that integrate artificial intelligence and blockchain technology. The National Combat Aircraft project, developed by TAI, features research on AI-driven combat capabilities. Blockchain will provide secure recording of flight data and ammunition management.

The convergence of blockchain technology with air power, autonomous systems, and robotics represents not merely an innovation, but a fundamental transformation of modern warfare doctrines. Conflicts such as the Nagorno-Karabakh War highlight the profound impact these technologies have on the trajectory of warfare.

These advancements, which facilitate secure, efficient, and ethical operations, are also shaping the geopolitical landscape. Nations that invest in these technologies will be pivotal in future conflicts and in maintaining global stability. The integration of blockchain with autonomous systems is not only advancing modern air power technologically but also addressing critical security and ethical challenges. We are no longer debating the adoption of these technologies but rather how swiftly and effectively we can implement them. The future of air power and warfare systems will be built upon these innovative technologies, which are now indispensable for complex systems and their integration. These projects aim to enhance operational efficiency by improving the traceability of aircraft component replacement and maintenance procedures.

Looking ahead to the future of security and cyber defence, air forces will need to leverage both artificial intelligence and blockchain technologies to ensure robust security and defence against evolving cyber threats. The integration of these two technologies, particularly within the cybersecurity domain, will be pivotal in safeguarding the Air Force's digital infrastructure.

The convergence of blockchain technology with air power, autonomous systems, and robotics represents not merely an innovation, but a fundamental transformation of modern warfare doctrines. Conflicts such as the Nagorno-Karabakh War highlight the profound impact these technologies have on the trajectory of warfare. These advancements, which facilitate secure, efficient, and ethical operations, are also shaping the geopolitical landscape. Nations that invest in these technologies will be pivotal in future conflicts and in maintaining global stability. The integration of blockchain with autonomous systems is not only advancing modern air power technologically but also addressing critical security and ethical challenges. We are no longer debating the adoption of these Technologies but rather how swiftly and effectively we can

implement them. The future of air power and warfare systems will be built upon these innovative technologies, which are now indispensable for complex systems and their integration.

For rapid deployment, my teams developing integrated solutions must possess in-depth expertise in command, control, communication, electronic warfare, reconnaissance, RF, thermal, optical, acoustic detection, sensors, war management methodologies, and weapon systems. However, to achieve this, we must first and foremost excel in fundamental sciences. We need to enhance our understanding and education in mathematics, physics, chemistry, and biology. I wish to emphasize that basic sciences should be addressed as a critical national security imperative.

Thank you.

QUESTION1: During your presentation, you mentioned that strategic superiority was achieved using unmanned aerial vehicles. While we might consider unmanned systems as a force multiplier in tactical scenarios, could you elaborate on how strategic superiority was attained? Furthermore, you referred to 'a new paradigm in air systems with autonomous systems.' Within this paradigm, what role do you envision for combat systems and manned systems?

ANSWER: My reference to the strategic superiority of unmanned aerial systems pertains to their enhanced data sharing, communication, and security capabilities. The strategic advantage lies in their ability to shift the dynamics of warfare, a transformation facilitated by blockchain technology. My intention was not to imply a traditional military strategic superiority. Regarding manned systems, they will remain essential in the foreseeable future. Technology augments human capabilities, and this is our focus. Specifically, in the realm of air power, we are exploring how blockchain can secure communications. Currently, GPS and signal jamming pose significant challenges, including for manned aircraft, and blockchain-based solutions are being developed to address these issues. The Air Force generates vast amounts of data, necessitating secure storage, transfer, and data integrity. Integrating blockchain with AI-driven systems will enhance

situational awareness for manned platforms. The distributed and decentralized nature of blockchain provides this security.

QUESTION 2: While blockchain technology offers a wide array of applications, its implementation in complex management structures presents challenges. Furthermore, its efficacy in data sharing or enhancing operational frameworks within a combat environment appears limited. What are your perspectives on this matter?

ANSWER: Numerous applications and projects are currently underway in this domain. Notably, DARPA is actively involved in projects utilizing Simbablok and Simbachain. While blockchain is often described as decentralized, this characteristic stems from its distributed architecture, not an inherent property. Consequently, given the distributed nature of both aircraft and unmanned aerial vehicles, I respectfully disagree with the assertion that blockchain's applicability is infeasible; it is indeed viable. Ongoing research and development efforts are dedicated to this area, including projects integrating quantum-enhanced blockchain technologies. The quantum computing domain is also being seamlessly integrated with blockchain. To abstain from these advancements would be akin to missing a crucial opportunity. The inherent distributed and decentralized nature of blockchain lends itself to these applications, as evidenced by existing projects. Furthermore, the integration of quantum computing with blockchain is being explored independently. Hesitation to embrace these technologies would result in significant missed opportunities. The distributed and decentralized attributes of blockchain demonstrate its suitability for these endeavors.

Dr. Marc LACY
LANCASTER UNIVERSITY
ENGLAND

Hello, people from my country usually only come to your country when it's very hot. So, it's a great privilege to see what your country is like in winter, and coming here reminds me that the food in your country is truly the best in the world. I'm very happy to be here. In terms of my work, I teach at Lancaster University, and I mentor students like my student Waqas Heider here. And I see myself as a defence anthropologist. Yes, I'm not from this country, and I spend my time talking to interesting people serving in armies all over the world, trying to create an interesting space for interesting conversations and dialogues between the military world and the academic world, and trying to talk about what can be done in this regard.

I'd like to share some insights from my book, which theorizes about the nature of future conflicts. The book is titled 'Theorizing Future Conflict: War to 2049.' The title alludes to 2049, the year China is purportedly aiming to rival the United States. While the US is often critiqued for its military strength, my book examines both sides of this equation. I delve into the trends that are likely to shape future wars, nations, and international relations. The book's opening chapter features a quote from science fiction author Douglas Adams, a favourite of Elon Musk, who describes future speculation as 'the stupid game.' Adams essentially argues that predicting the future is a futile endeavor. Yet, despite its inherent challenges, we must engage in this exercise. In this presentation, I will attempt to raise several questions about the complexities of future-oriented thinking and planning, acknowledging that contemplating the future is indeed 'a stupid game.

The concept of living in an era of proliferation is something I find quite compelling. Back when I was an international relations student in the 1990s, Fukuyama proposed that there was only one path for the future, which was fundamentally liberal democracy.

My perspective on the future was entirely uncritical.

So, how exactly will this 'end of history' scenario unfold? We didn't anticipate the rise of China. We didn't foresee this impending era of rapid technological advancement. We were naive, and perhaps we will always be when contemplating the future. We can be naive when considering the future; I certainly believe we were quite naive during our university years in the UK and America in the 1990s. Therefore, my central argument is that we are, in fact, living through multiple futures, multiple possibilities, in a time of manifold potentialities. This is an era of proliferation, and to illustrate what this proliferation entails, we are witnessing a surge in actors and actions unlike anything we've encountered before, and we are glimpsing a multitude of possible futures.

Consider Elon Musk, for example, a truly global actor. By mid-century, we may well witness the emergence of ten more individuals like him, wielding significant global influence across diverse sectors such as Artificial Intelligence, neuralink, and space exploration. These figures may hail from China, India, or other unexpected corners of the globe. In this age of open technological innovation, we will see a proliferation of non-state actors operating concurrently. These actors will possess highly sophisticated capabilities, intelligence, and potentially dangerous agendas. Therefore, we must anticipate that a diverse array of actors, each with unique capabilities, will be capable of undertaking a wide range of activities. We will see new architectural spaces emerge in space, underwater, and within the metaverse.

For instance, is the Neom project in Saudi Arabia a pioneering initiative for novel urban concepts? Will neuro warfare, a form of cognitive conflict currently under discussion, represent a new frontier in warfare? And it may become necessary to recognize this cognitive warfare domain as a legitimate military theater. You will find yourselves conducting military operations in novel domains that currently do not fall under traditional military classifications. As operations expand into these areas, we will witness a proliferation of tools in domains like quantum computing and nanotechnology, encompassing unmanned aerial vehicles, robotics, and cyber warfare.

The proliferation of new tools and a constantly evolving world will pose significant challenges for any organization. In UK universities, we're grappling with the complexities of how students utilize artificial intelligence, and we must adapt accordingly. Similarly, military organizations will need to keep pace with an expanding array of technologies and tools, necessitating robust organizational structures and meticulous planning.

Technological prowess necessitates corresponding human skills and capabilities. The 'granularity' or 'level of detail' of conflict, as I discuss in my book, implies that we will possess technologies of diverse shapes and sizes. For instance, consider the implications of unmanned aerial vehicles of varying dimensions and how they will reshape the conflict landscape. We will witness a proliferation of tactics, a surge in threats akin to those observed in hybrid warfare, and an increase in ecological threats. Moreover, the repercussions of these conflicts remain uncertain. While the full extent of climate change's impact on the planet is unknown, I anticipate it will have devastating and transformative consequences.

An individual from the British Army discussed certain technologies familiar to you, highlighting that some tanks and combat vehicles are not designed for specific climatic conditions, leading to operational challenges. Should your technology prove unsuitable for potential climatic scenarios, its effectiveness may be compromised. We can explore the proliferation of diverse political futures, the types of conflicts that multipolarity may engender in the context of war and peace, and ultimately, the proliferation of futures that entail the transformation of the human body and the very definition of humanity.

For instance, what will neuralink technology entail? How will the concept of cybernetic organisms, encompassing cyborgs and robotic enhancements, transform our understanding of humanity? Can we foresee how these advancements will reshape the human soldier, at the fundamental level of flesh and blood? In essence, we are contemplating a multitude of possibilities, engaging in what Douglas Adams termed a 'stupid game' as we attempt to discern the future. This is the context, this is the challenge before us. Naturally, there are numerous

other avenues for comprehending our trajectory, and additional factors to consider. However, two pivotal organizational challenges emerge when envisioning the future soldier.

In discussing the concept of a New World, New War, and New Warrior, I propose that we should pluralize these terms and consider the notion of New Worlds, New Wars, and New Warriors. Which worlds, wars, and warriors will we confront? I believe there are two principal approaches to addressing this question. Nassim Nicholas Taleb's book, 'The Black Swan: The Impact of the Highly Improbable,' has had a profound influence in both the United States and the United Kingdom. In the UK, particularly within the Ministry of defence, the concept of a 'Black Swan' event is of paramount importance.

Essentially, a Black Swan event is something that should have been foreseeable, yet it remains unseen and unpredictable. This concept is the subject of considerable debate in the United States. While 9/11 was considered a Black Swan event for America, the pandemic was not, as it had been extensively discussed beforehand. Thus, there are events that should have been anticipated but were overlooked. Taleb argues in his book that the interconnectedness of our world will lead to an increased frequency of Black Swan events in the 21st century. He emphasizes that organizations often fail to recognize these events due to 'tunneling,' a phenomenon where they develop a narrow perspective. For instance, in my experience working within a bureaucratic university organization, we frequently devise unorthodox strategies to convene key individuals and innovate processes, as those in leadership positions often lack a comprehensive understanding of the realities faced at lower levels.

I consistently advise those seeking to comprehend organizational dynamics to engage with secretaries and communication personnel, as they often possess a more nuanced understanding of operational realities. While senior leadership may espouse innovative ideas and business philosophies, they frequently lack the granular insight into day-to-day operations. I believe that bureaucracies, organizations, and institutions should adopt a more detailed approach to problem-solving. For instance, the UK Ministry of defence faces

the challenge of multiplicity, necessitating a strategy to adapt to this complexity. A comprehensive understanding of emerging technological domains, including artificial intelligence, as well as relevant industries, trends, and scientific advancements, is paramount.

To effectively plan for the Future Soldier, I believe certain measures are essential. Firstly, ensure that your processes facilitate robust discussions and diverse perspectives. While engaging with senior management is crucial, when addressing domains like cyber warfare, it may be necessary to involve younger experts, such as 20-year-old hackers, who possess invaluable insights. They are often more adept at understanding and adapting to emerging trends compared to those over 25-30. We are all aware of the challenges associated with keeping pace with innovation. Secondly, I draw upon the work of French writer and philosopher Paul Virilio, who extensively explored the concepts of speed and acceleration in warfare. He argued that warfare has undergone a transformation in the 21st century, blurring the lines between war and peace. He posited that pure war, in the traditional sense, no longer exists, and instead, we are confronted with a state he termed 'impure pure war.'

Now, it is qualified with words like gray zone or hybrid warfare, but his argument is that one of the biggest challenges in our technological societies in the 21st century will be technological accidents. His argument is that any new technology can lead to a new type of accident and possibly global accidents or accidents. There are many technological companies in the world we live in and there are many new technologies that are sold to you with optimistic visions of how to improve things. But Virilio directs you to look at what kind of accident this new technology can create. Because there will always be a 'Black Swan' event, whether it is the military or the university, accidents caused by new technologies that all organizations buy, you should also include in your processes ways of thinking about accidents that may occur in the processes you started to make things efficient. Because every new technology that promises progress carries the potential for a new and unprecedented type of accident. These kinds of concerns will be more important in the future.

We are witnessing the emergence of a striking duality with artificial intelligence and human-machine collaboration. While advancements in AI are promising, they also present significant threats. I frequently discuss with my students the growing issue of plagiarism facilitated by AI tools like ChatGPT. Although these tools make writing more accessible, we also leverage AI to detect instances of plagiarism. For instance, last year, AI generated a reference for a book that an academic had never authored. We must now consider the military implications of such errors.

The issue of trust is paramount here. If you envision human-machine teaming, you must also consider the potential for accidents and the challenges to trust. The pager attack in Lebanon is a prime example illustrating my point. Regarding drones and AI, there's a quote that encapsulates much of my thinking on these matters. In the late 1990s, the Chinese book 'Unrestricted Warfare' explored future warfare trends and the technological transformation of information warfare. Within its pages, the Chinese authors state, and I quote in my own book, 'What we must say, then, is that the new concept of warfare will cause ordinary people and soldiers alike to experience great astonishment upon realizing that everyday objects, familiar to them, can be transformed into weapons of war. We believe that one morning, they will awaken in astonishment to discover that these seemingly innocuous items have become formidable weapons. They will be astounded to find that many benign and beneficial things possess aggressive and lethal capabilities……"

These lines essentially illustrate how ordinary items can be weaponized. Therefore, returning to the 'Black Swan' theory, we must consider which everyday objects could be transformed into weapons and used against us, and what the potential methods might be. In the realm of international politics, there was a hierarchical structure dominated by the United States and the Soviet Union. This structure provided a clear framework for military development, with established expertise and budget allocations. However, I believe that technology has fundamentally disrupted this paradigm.

The military of the future must be prepared by anticipating the realities their adversaries will face. For instance, the operational environment will be so dynamic that the ability to

adapt and respond will be a constant topic of discussion. Your rivals will capitalize on open technological innovations, as previously mentioned. We are witnessing the global impact of drone technology, a prime example of open technological innovation. We see how these technologies are being deployed as they become more affordable, powerful, and agile.

Thank you for listening to me.

QUESTION: What will be the most crucial determinant in the battlefields of the future?

ANSWER: There are tactics of many actors. Technologies and the asymmetric dimension, these are a big headache for America and world powers. With artificial intelligence, your enemies can now become invisible, do things that will surprise you, and you will have to be constantly vigilant, this is the basic challenge for all actors. The war processes from now on are about who will be the most original, who can create the most different. As much as you have a lot of different tools, your success will be about what you can achieve the most different in this chaotic environment. You can do a lot with access to these tools, but that doesn't mean you know how to use them most efficiently and originally. So being able to do the best by controlling everything for your structure is the most important, whether you are the Pentagon or a drug cartel. I think creativity, originality and being able to do the best is the biggest challenge of the new war era.

Muhammed Waqas HAIDER
LANCASTER UNIVERSİTY
ENGLAND

Hello dear ladies and gentlemen, esteemed colleagues and distinguished authorities, Dr. Mark Lacy, in his book 'Theorizing Future Conflict: War to 2049,' discusses by theorizing future conflict.

The future will most likely be a time of proliferation. A time of proliferation of tactics, terrains, technologies and actors. The onset of future wars will likely occur within a complex environment, marked by the challenges and disruptions of both traditional and novel warfare. These settings will be characterized by a blend of proven and unproven tactics, as well as the integration of experimental and established practices.

The effectiveness and feasibility of innovative tactics will be tested on the battlefield, where the impact will be subject to unforeseen outcomes. Throughout history, the conduct of war and its innovations have been shaped by various eras, from ancient Greece to medieval Europe, with the advent of cavalry and tanks...

Each technological advancement has fundamentally transformed not only the conduct of warfare but also redefined doctrines, strategies, and even geopolitics. Picture a contemporary battlefield where human decision-making alone is insufficient in speed and accuracy, a sky teeming with drone swarms, sophisticated communication networks, and soldiers equipped with adaptive technologies. Envision environments where technological exoskeletons and augmented reality displays are commonplace, where data, not just projectiles, dictates survival—and recognize that this is not a distant vision. The reality of the conflict between Russia and Ukraine has become a stark illustration of the current state of technological warfare. The modern battlefield is a crucible where innovation and destruction converge, reshaping the very essence of how wars are fought and won. This conflict serves as a global laboratory for testing disruptive technologies that are reshaping military doctrines and influencing the future.

It reshapes military doctrines and also affects global strategies in the development of future technologies.

The strategies employed in this conflict have demonstrated that disruptive technologies not only transform tactical approaches but also significantly amplify their impact. Furthermore, they have raised profound ethical questions regarding warfare. Our discussion will primarily focus on providing a background on the evolution of warfare in the 21st century, followed by an examination of the scope of disruptive technologies and their role in reshaping future discourse. We will provide a global overview of future military programs and explore the contemporary operational concepts that integrate autonomous military technologies.

Human history is an integral part of human interaction at various levels of society, with war and wars. Land and sea wars were the primary areas of combat struggle where we gained a lot of experience, at the beginning of the 20th century, we saw the introduction of air power and the game-changing form of conflict in the field of technology. We have seen that it has been reshaped, especially recently. We also saw your effect in the Nagorno-Karabakh War. Now we are stepping into space and cyber. Although they are not new, they are now developing at a very fast pace. And as a technology, we are becoming more dependent on these two areas, which are really very comprehensive, than others.

It is emphasized that the 21st century global security landscape is marked by challenges posed by both state and non-state actors. Furthermore, they are adapting and adopting each other's tactics and tools for counter-warfare.

At this point, 'Dragons and Snakes,' David Kilcullen highlights that despite their distinct origins, both state and non-state actors are pursuing their objectives with similar tactics. He contends that state actors, or 'dragons,' are learning from non-state actors, or 'snakes,' and conversely, that the dragons' methods are being adopted to combat the snakes. Kilcullen argues that we are now witnessing unprecedented combinations of state and non-state threats in emerging domains. Consequently, we are seeing the emergence of novel battlefields and forms of warfare. The global conflict landscape

is becoming increasingly complex, with the introduction of previously unseen and unanticipated methods.

Mark Galeotti, in his book 'The Weaponization of Everything: A Field Guide to the New Way of War: The Unprecedented Interconnectedness of the Modern World,' emphasizes the unprecedented interconnectedness of the modern world, states that innovations enable new methods in wars, and highlights that they enable new war methods through cyber, space and the electromagnetic spectrum.

Ben Zweibelson, drawing from US Space Command studies, categorizes warfare into three distinct eras: pre-modern, modern, and ghost war. Pre-modern warfare is characterized by its reliance on ideologies, mythological beliefs, and cultural systems, which he terms 'supernatural rationalization.' Modern warfare, on the other hand, is defined by human-centered rationalization, where decisions are made through various tools and technologies, marking the scientific age. While some argue that contemporary conflicts remain within the realm of modern warfare, the convergence of domains like space, artificial intelligence, and cyber warfare, coupled with the involvement of special forces, is ushering in a 'ghost war' paradigm. This new era of warfare is characterized by the technological augmentation of humans and the redesign of advanced weaponry, creating a scenario where human control may be circumvented within decision-making cycles.

One of the perceived dangers of artificial intelligence is its potential to operate outside of human decision-making loops. While humans traditionally remained within these loops, there is now a possibility for AI to transcend them. This era, termed 'ghost war,' is characterized by the conceptualization of advanced weaponry that can autonomously redefine its objectives, surpassing human control. It represents a period of technological transcendence. Humans are no longer in full control of decision-making cycles; they can only conceptualize and adapt to technologically augmented conflicts. A ghost war introduces a paradigm shift, distinct from all forms of warfare, both conventional and unconventional (regular and irregular, symmetrical and asymmetrical). I'd like to discuss the application of disruptive technologies in the Russia-Ukraine

War. From both a practical and academic standpoint, we'll examine their influence on evolving strategies.

The Ukraine conflict has vividly illustrated the shifting strategies and dimensions of modern warfare. Turkish-made Unmanned Aerial Vehicles (UAVs) have been extensively utilized in this conflict. The TB2 Bayraktar, in particular, played a crucial role during the initial stages of the war, compelling the Russian Air Force to redeploy its defences and units to counter these systems. This highlights the transformative impact of technology on the structure of warfare. Significant advancements have been made since the Nagorno-Karabakh War, with the development of diverse munitions. Russia has introduced the Kub-BLA, a high-precision UAV and loitering munition, capable of autonomous target detection and engagement. These systems align with the latest trends in autonomous weaponry, leveling the playing field by enhancing the competitiveness of smaller units against larger adversaries. These technologies are becoming increasingly affordable and accessible, extending beyond traditional military powers.

The conflict in Ukraine has also demonstrated the integration of artificial intelligence into battlefield analysis and accelerated decision-making. Regardless of the operational domain, AI has been employed to analyze battlefield data, including satellite and reconnaissance imagery, for observation, targeting, decision support, and preemptive action. This has enhanced the targeting of Russian forces and streamlined decision-making processes. Ukraine has also utilized Clearview AI's facial recognition technology to identify Russian soldiers, including prisoners of war and casualties.

Artificial intelligence-driven identification, which blurs the distinction between warfare and personal security, has been trialed in combat scenarios. In essence, AI-enabled identification technologies blur the lines between military operations and individual privacy by enhancing operational efficiency and reducing the time gap between intelligence collection and technical deployment. These software applications exemplify the ethical and operational dilemmas inherent in contemporary artificial intelligence. These give us important ideas about the battlefields of the 21st century with new technologies. In addition, new Technologies are used in

battlefields and post-war field reporting. For example, Russia deployed the Uran-9, a robotic combat vehicle, for reconnaissance and fire support.

While facing some operational challenges, it was tested to reduce human casualties on the battlefield, showing us some clues about what robots promise and an indication of increased reliance on robotics in high-risk scenarios. There is a long way to go in reducing human casualties while maintaining effectiveness in the field, but we can also see that they will create a revolution in this area.

At the same time, Blockchain also contributed to war finance. Support was given to Ukraine to receive international donations and to finance sustainability to cope with Russian attacks. These types of financial systems offer an alternative to traditional banking, especially when countries are under economic sanctions. This system helped both countries because while aid was given to Ukraine, it also provided alternative economic ways for Russia's embargoed banking system.

Concurrently, both nations are deploying quantum-resistant technologies. Quantum technologies have provided support in areas such as communication, safeguarding sensitive data, and counter-espionage. 1 The High Mobility Artillery Rocket System (HIMARS) has enabled Ukraine to conduct precision strikes against Russian ammunition depots and command centers. 2 Additionally, the portable and highly effective MGM 140 and Storm Shadow air-to-air army tactical missile systems, along with Javelin anti-tank guided missiles, have empowered small infantry units to effectively engage heavily armored Russian tanks.

Anti-armor missiles have been instrumental throughout the conflict. Hypersonic missiles also serve as a key indicator of technological advancement. What, then, do smart technologies accomplish? The ability to precisely target objectives, coupled with extended strike ranges and devastating effects, has revolutionized artillery. In recent times, satellite and space-based technologies have also exerted a significant influence. During communication disruptions in Ukraine, Starlink satellites were activated, and while Ukraine utilized this technology, there

are reports suggesting that Russia also employed it. At this point, we see how the balance is used when this technology is used by both powers, in case there are non-state actors doing these kinds of things. We also see the importance of balance. This highlighted the role of privately owned, space-based technologies in maintaining strategic communication in contested areas by multiple actors.

Cyberwarfare and information operations have played a significant role in this conflict. Russian state-sponsored hackers have launched cyber-attacks targeting critical infrastructure in Ukraine, including power grids and financial systems. The attack on Ukraine's power grid was particularly noteworthy. In response, Ukraine mobilized volunteers globally to form the 'IT Army of Ukraine,' focusing on disrupting the websites, communication systems, and propaganda networks of the Russian government. The cyber domain is a hive of activity, and operations within the cyber battlespace are of paramount importance. These events demonstrate the seamless integration of the digital and physical worlds and their associated consequences. The proliferation of cyber warfare capabilities enables smaller nations to inflict significant damage upon much larger adversaries.

Electronic warfare played a crucial role in the Russia-Ukraine War. Russia employed GPS jamming to disrupt Ukrainian navigation and targeting systems. Ukraine's Anti-Drone Electronic Warfare Systems proved effective in neutralizing Russian drones mid-flight. We observed a rapid cycle of new defence technology development in response to each attack. This included the identification of vulnerabilities in spectrum technology, the detection of weaknesses, and the deployment of counter-technologies.

Social media and open-source intelligence (OSINT) have assumed a profoundly strategic role in this conflict. Platforms like Twitter, Telegram, and TikTok have transformed into real-time intelligence hubs, with citizens sharing information on troop movements and military activities. Memetic warfare has also been employed, with both sides utilizing memes and viral content to sway public opinion and undermine enemy morale, thereby establishing a novel form of psychological warfare. While publicly available data augments traditional espionage,

the rapidity and extensive reach of digital platforms have amplified the psychological effects of propaganda campaigns. Beyond traditional espionage, real-time access to information has amplified and complemented the speed and scope of digital intelligence gathering.

In light of all these developments, the soldier of the future will be a soldier focused on changing technologies.
They use smart helmets, displays with augmented reality and data access. Soldiers equipped with these technologies access real-time battlefield information. They access much more data, including maps, threats and mission objectives, with much less communication. This allows them to have instant situational awareness of the war and make faster decisions. The American Army, for example, attaches great importance to programs such as visual enhancement systems. Nations are investing in exoskeleton technology to reduce fatigue and increase endurance. It has also been revealed that this technology is vital in urban warfare scenarios, as evidenced in the Ukraine conflict. You need mobility, flexibility and protection in an urban environment. Therefore, these kinds of programs receive a lot of funding and a lot of research is being done in this area. Gene and cognitive enhancements are becoming very important. There are studies to improve people's physical and cognitive abilities and increase their situational awareness with genes or enhancement technologies. Ethical issues are discussed on the one hand, but biotechnology is also a popular topic to increase operational capabilities.

These advanced technologies, including sophisticated robotics and autonomous systems, are designed to augment the capabilities of human soldiers. Robotic carriers support logistical operations, while combat robots are deployed for reconnaissance and assault. Of course, all of these systems require highly skilled and trained personnel. These elements function in an integrated environment, where they mutually reinforce each other.

The future soldier describes not only capability, but also an operational system that is fully integrated in a larger area, powered by artificial intelligence and network solutions. Networked soldiers are integrated into a larger data network system with more powerful sensors, and with these software,

technology provides instant decision-making and situational awareness during conflict. In America, the 'Joint All-Domain Command and Control (JADC2)' system is being developed to supervise all this command and control area. This system endeavors to establish a preemptive warfighting capability, enabling action before the adversary can react, while fostering an interoperable environment across all domains.

It aims to achieve coordinated operations across the five conflict domains: Air, Land, Sea, Cyber, and Space. Analytical machine learning and artificial intelligence are leveraged to ensure the equitable and timely deployment of all available assets. These technologies, powered by AI, are fundamentally reshaping the nature of conflict, as evidenced in Ukraine.

Autonomous systems and integrated operations are fundamental to the future of warfare, as evidenced by the conflict between Ukraine and Russia. Autonomy, ranging from loitering munitions to drone warfare, minimizes human risk and enhances operational flexibility. Integrated operations utilize the 'war cloud,' a system that consolidates data from satellites, drones, soldiers, and sensors in real-time to inform decision-making. Technologies like Starlink showcase the ability of decentralized, redundant systems to maintain operational continuity, even when faced with adversary attempts to disrupt infrastructure.

Contemporary warfare transcends traditional land, sea, and air domains, encompassing cyber and space. Integrated strategies facilitate the synergistic operation of these domains. Artificial intelligence (AI) serves as the linchpin of this integration, providing predictive analytics, automated decision-making, and strategic foresight. The swift adoption of AI-enabled systems in the Ukraine conflict highlights their critical importance.

As autonomous systems take on more decision-making roles, who is held accountable for unwanted or unethical actions, such as programmers, operators, or governments? How can we ensure transparency in these systems? This is the question we need to ask ourselves. Then, integration needs to be ensured. While the integration of technologies such as artificial intelligence, unmanned aerial vehicles, and satellite

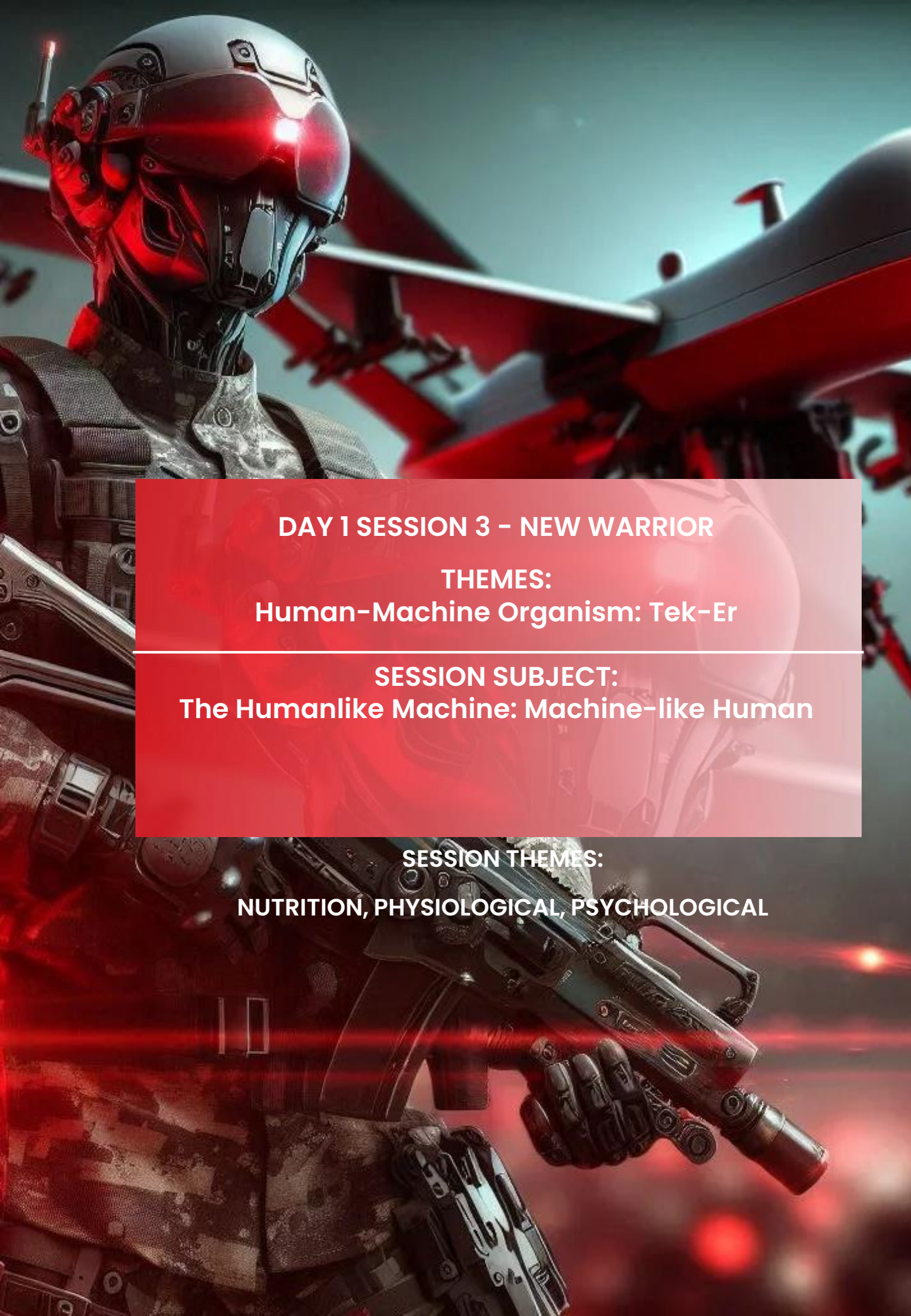
systems increases battlefield efficiency, it also leads to dependencies. What happens if these systems are compromised or neutralized by adversaries? Can traditional doctrines designed for industrial age warfare be adapted to the demands of modern, technology-driven conflicts? What should be the role of human oversight in such doctrines? Are we shaping technology to serve the principles of fair and ethical warfare, or is technology turning war into something we can no longer control? This is the critical juncture at which global society stands today. I urge you to consider not only how we use these tools, but also how they shape the human and geopolitical narratives of tomorrow's conflicts.

Thank you, best regards.

QUESTION: The soldiers were wearing such clothes in the presentation that they no longer looked like humans, but rather humanoid. It seemed exaggerated to me, can they even walk? For example, in the last Olympics, our National shooter Yusuf Dikeç succeeded without wearing any special clothes. Can you evaluate this? How will a soldier move like that in the operational area?

ANSWER: There are many programs followed by different countries in this field. Under the title of future soldiers and warriors. What is being tried to be done there is as if there is a robotic side, but you are developing human abilities and giving robotic features. Basically, you are trying to empower the human. For example, when you add enhanced display screens and artificial intelligence, what you see improves and becomes more meaningful. Your situational awareness in that environment increases with real-time images from all sensors. They wear external or supplementary skeletal systems, a kind of bionic motorized or electric facilitators. This increases your carrying capacity, mobility and reduces your burden. In previous wars, warriors who wore shields and those who wore things that increased weight also reduced their mobility. New technologies, on the other hand, increase their mobility. Genetic changes and biotechnologies are also similar development programs related to the human body. Of course, ethical evaluations are made, we will have to see how these programs will take shape in the future, but these kinds of things are being

done right now and what is important is that there are programs to protect, care for, and make the military more active, and that we need to prepare for this. These technologies are made to make the military more ready for urban warfare environments.



DAY 1 SESSION 3 - NEW WARRIOR

THEMES:
Human-Machine Organism: Tek-Er

SESSION SUBJECT:
The Humanlike Machine: Machine-like Human

SESSION THEMES:

NUTRITION, PHYSIOLOGICAL, PSYCHOLOGICAL

THIRD SESSION SUMMARY

Systems that ensure soldiers' tracking and sense of security in the field in the face of developing technologies are important. The needs of the Single-Soldier for developing war conditions need to be planned correctly and their adaptation to new technologies should be ensured in terms of field management. Especially capabilities for defence against explosive or unmanned systems should be developed.

NATO's near-term warfighting perspective emphasizes that, despite technological advancements, critical decision-making will remain with humans for the foreseeable future. This perspective also highlights the integration of manned and unmanned systems. The focus on technology enabling the seamless and integrated operation of air, sea, land, cyber, and space domains reflects NATO's technology outlook for the near and medium term.

Combat pilots significantly influence the trajectory of warfare through their decisive actions, particularly in the lead-up to ground operations, where their individual expertise, intelligence, situational awareness, and problem-solving skills can prove pivotal. The increasing reliance on technology places a substantial cognitive burden on these pilots, underscoring the growing importance of selecting and training personnel capable of managing this load.

Technology-induced sedentary behavior poses a significant challenge to personnel agility and responsiveness. Physical energy levels play a crucial role in determining mobility, strength, and endurance, particularly during soldiers' adaptation to technological equipment. Tailored training and nutritional programs are essential to address individual needs. Specialized training and practical load-bearing exercises are particularly vital for special forces and personnel operating remote systems.

Modern warfare is increasingly focused on rapid response and reaction speed, rather than traditional endurance. It's crucial to thoroughly analyze the implications of emerging technologies, understand their impact on soldiers, and adapt training programs accordingly.

Oğuz Alpay AYDIN
SECRETARIAT OF DEFENCE INDUSTRY (SSB)
MODERATOR

Greetings and welcome to everyone. In this episode, we will delve into the fascinating topic of the 'Human-Machine Organism,' and we will explore an intriguing concept: the humanoid machine and the machine-like human. We will cover a range of subjects, including power, speed, endurance, psychology, decision-making processes, nutrition, physiology, and adaptation to technology.

Ömer DOĞAN
ASELSAN

Greetings, today I will endeavor to offer a command and control perspective on human-machine interaction. ASELSAN has been dedicated to the 'Future Soldier' concept for many years. We are actively developing solutions for the integration of evolving technologies into the combat environment within the context of human-machine collaboration. Our CENKER system is designed to address the command, control, communication, situational CENKER is a system designed to enhance the overall combat effectiveness of soldiers, from individual units to larger formations like corps, brigades, and battalions, by providing essential command, control, intelligence, logistics, communication, situational awareness, and coordination capabilities within a digital network framework. This system has been under development and field-tested in combat environments for the past three years. We are meticulous in our design process, ensuring that technological advancements are balanced with the cognitive demands placed on soldiers. While technology offers immense potential, it must be practical and relevant to the realities of the battlefield. Our development process benefits from the expertise of retired military personnel and experienced military specialists. We are also engaged in collaborative efforts with NATO, and we actively incorporate feedback from end-users in the field to refine and improve our

system. The paramount requirement in the field is to accurately identify and address the genuine needs of personnel. On the battlefield, personal water consumption is a critical concern. Ideally, soldiers should consume 3 liters of water daily under normal circumstances. Command and control systems facilitate the planning of water quantities carried by personnel, considering climatic conditions. Water consumption drills, from training to field operations, instill habits of water conservation. Ensuring adequate food and beverage variety, along with lightweight and portable provisions, is essential. Collaboration with command and control is crucial for monitoring soldier health, issuing alerts for inadequate nutrition and water intake, and facilitating the use of supplies. We also develop solutions for the accurate planning and effective management of warriors' needs on the battlefield.

During operations, a collaborative framework is established between soldiers and command control to manage this process effectively. Soldiers require approximately 4,000 calories daily, a need that can be monitored and managed in the field through the CENKER system, in coordination with the command control center and the soldier. In urgent or exceptional circumstances, issues can be reported and resolved through the system. The system also includes features designed to alleviate feelings of isolation among soldiers, foster a secure environment, provide support from their unit and senior commanders, and mitigate the impact of excessive stress, fatigue, attention deficits, and diminished perceptual abilities. The CENKER system simplifies target identification, promotes clear and concise information management, prevents information overload, enhances command and control capabilities for small unit leaders, facilitates communication through text, graphics, templates, and multimedia tools, and contributes to overall well-being with remote health support.

The CENKER system is designed and continuously enhanced to provide a wide range of functionalities, including: real-time monitoring of soldiers' health data, early warning alerts, notifications for CBRN and artillery attacks, secure route tracking, incident and situation updates, information dissemination to command centers, marking of critical points and areas, target detection and alerts, laser and touchscreen -

based target warnings, team member status updates, individual and team alerts, hazardous area warnings, and information flow for unmanned systems operations. The system includes capabilities for providing alerts against unmanned systems operating in the area. Furthermore, the system is being enhanced to encompass features related to both real-world and simulated systems, accommodating multi-domain actors and capabilities. Ongoing development efforts focus on areas such as mine detection and clearance, load reduction through auxiliary carrying systems, basic energy generation for battery-powered devices, and data utilization for post-action reviews and new planning initiatives. We are actively pursuing enhancements and research to develop a system that aligns with next-generation multi-domain integration and advanced command and control frameworks. In closing, as you are aware, TUSAŞ was recently subjected to an attack, resulting in the loss of heroic lives who were fighting on our behalf. May the souls of all our fallen martyrs find eternal peace.

QUESTION: Observing global military literature and modern armed forces, we note a transformation in command and control architectures. Specifically, the integration of Artificial Intelligence and other advanced technologies is driving the development of autonomous and hybrid control centers. I would appreciate your insights on this trend: Is it a consistent evolution? And to what degree can autonomy be implemented?

ANSWER: We recently participated in a NATO event focusing on 'Multi-Domain Operations,' where we observed a significant emphasis on these concepts. Our key takeaway was that NATO anticipates a shift towards: delegating routine decision-making to autonomous systems and machines, while reserving high-value, strategic decisions for human operators. Consequently, NATO is actively engaged in discussions regarding autonomous decision-making, the utilization of these systems for accelerated decision cycles, and the seamless integration of manned and unmanned platforms. To alleviate the cognitive burden on human personnel, machines will be entrusted with lower-level decisions. Furthermore, to streamline the interoperability of land, sea, and air systems, these integrated platforms will likely be equipped with autonomous decision-making capabilities, reducing the need for human intervention in technical minutiae.

Dr. Major Rıfat UĞURLUTAN
Turkish Air Force (HUGEM)

Major Uğurlutan, permission to speak, sir. I will present to you the research we have conducted at the HUGEM Command within the Air Force, focusing on human augmentation systems. To begin, I'd like to reference a podcast discussing the Ukraine-Russia War, a conflict occurring in our immediate vicinity. In this broadcast, titled "What the Ukraine-Russia war teaches us about air and space power," two senior NATO commanders highlight the critical role of air superiority in shaping the outcome of the conflict in Ukraine.

The lack of established air superiority significantly hinders the efficacy of ground operations. In this context, it has been observed that the absence of air dominance transforms ground operations into a protracted exchange of missile and rocket fire, with neither side gaining a decisive advantage. This underscores the pivotal role of combat pilots as a critical force multiplier on the battlefield. Beyond merely operating sophisticated aircraft, these pilots leverage their inherent intelligence, situational awareness, and innovative problem-solving skills to fundamentally alter the course of conflict. Combat pilots, as previously mentioned, orchestrate a symphony of destruction with their aircraft, and the instruments of this symphony are constantly being augmented. Notably, even with the advent of 6th generation technologies, the role of the pilot remains indispensable. From a neuroscience perspective, artificial intelligence should be viewed as a collaborative tool, not a competitive adversary. Its optimal application lies in refining and enhancing human capabilities. Interestingly, when prompted, AI itself depicts a pilot wielding a weapon, emphasizing the human element as the ultimate arbiter of warfare. While we continue to develop increasingly advanced machines, a system designed to operate at 50,000 feet is ultimately limited by the human pilot's physiological constraints, such as the need for oxygen, which restricts them to 25,000 feet. The US Air Force has tasked NASA with addressing this critical challenge.

We now understand that the scope of pilot training and flight physiology extends beyond mere physical demands, encompassing the significant cognitive challenges that arise. Consider, for instance, the stark contrast between the rudimentary aircraft of World War I, lacking even a canopy, and the sophisticated technology of modern aviation. While pilots of the past primarily required equestrian skills, we now employ specialized assessments to evaluate both mental and psychological fitness. Furthermore, pilots must now communicate not only with their own aircraft but also with a multitude of airborne entities, ultimately determining the optimal weapon deployment for each. In the past, the question was simply, which of these individuals had the aptitude to become a pilot? Today, we recognize that successful pilots must possess a blend of intellectual curiosity and resourceful problem-solving skills.

In its recent report, NATO has identified biotechnology as one of seven key areas, with a particular focus on neurotechnology and research aimed at enhancing human performance. When discussing neurotechnology, it's essential to acknowledge the critical role of nerves and neuroscience in shaping future technological advancements. However, there's a prevailing misconception among neuroscientists that neurons are simple structures. In 1981, we discovered that Cajal neurons exhibit diverse and intricate morphologies. This complex architecture comprises numerous components, with the cell body serving as the neuron's central hub. It is within the cell body that proteins are synthesized, initiating the neuron's functional activity. The dendrites, which facilitate communication with other neurons, play a crucial role in preparing the neuron for its active or future state. This preparation can involve either excitation or inhibition. We characterize neuronal information transmission through an electrical phenomenon known as the action potential.

What exactly is this action potential? In a resting neuron, the exterior environment exhibits a positive charge. This positive charge migrates inward, establishing a chemotactic electrical potential. This electrical potential is the foundation of what we refer to as 'brain waves' when we measure brain activity. This phenomenon arises from a simple ion exchange within the neuron. However, this process is far from simplistic.

The synapse, the junction between an axon and a dendrite, features an area known to quantum physicists as a quark. It is within this synaptic space that information transfer and exchange occur.As a result of this information exchange, neurons mutually enhance their capabilities and establish interconnections. Neurons engage in the transfer of information between one another. To perform a task, a neuron forms a connection or relationship with another neuron. So, how do we measure these changes in electrical potential using this method? Through scientific techniques, we can access the brain of a living organism, probe a specific neuron, and measure the electrical or chemical variations occurring within it. Neurons, through their continuous communication, collectively construct the brain.

The brain is a highly specialized organ, adept at simultaneously managing diverse functions across various regions. For example, the frontal lobe plays a crucial role in executive decision-making, distinguishing us from other primates. The temporal lobe is primarily responsible for auditory processing and memory functions. The brain stem, another vital component, governs essential physiological processes, such as respiration and cardiac activity. So, are complex systems always required for measuring brain activity in humans? No, we can utilize techniques like electroencephalography (EEG), a multi-channel voltmeter-like system, to analyze these changes and monitor neuronal activity. Furthermore, functional near-infrared spectroscopy (fNIRS) enables us to assess the brain's energy expenditure and function by quantifying oxygen consumption during specific tasks.

There are indeed variations in brain structure and function between individuals, and certain traits are present from birth. The male brain typically weighs around 1400 grams and comprises approximately 100 billion neurons, while the female brain weighs about 1300 grams and contains 90 billion neurons. While it may seem logical to assume that men are more intelligent due to having more neurons, this is not necessarily the case. The female brain is more compact and exhibits capabilities that may exceed male cognitive functions. To illustrate this point, in 2005, Lucy Brown conducted an MRI study to examine brain activity in men and women when viewing

photographs of the opposite sex. The study revealed no frontal lobe activity in men.

What does this imply? Men, it seems, are primarily focused on physical appearance, while women engage their frontal lobes, contemplating the nature of their potential relationship, its economic implications, and the level of care they will receive. Can education induce cerebral changes in individuals? To explore this, let's examine the case of Albert Einstein, the only person in the world whose brain was stolen.

Upon examination of his brain, it was observed that the corpus callosum, the structure facilitating communication between the right and left hemispheres, was significantly more developed. Additionally, the postcentral gyrus, the region associated with complex mathematical processing, exhibited a larger size.

What, then, is the brain's capacity for processing information? We refer to this as cognitive load. Cognitive load is a dynamic concept, influenced by an individual's inherent abilities, external stimuli, and the complexity of the task at hand. In 1988, Dr. John Sweller introduced the Cognitive Load Theory, which explores the limitations of the brain's information processing capacity during learning. You have a certain capacity to manage something, there is a load that an instructor puts on you, and whether you can break down and digest this event is the question. Intrinsic load refers to the inherent difficulty of the material itself, extraneous load encompasses extraneous factors that may hinder or aid learning, and germane load pertains to the cognitive effort devoted to constructing and automating schemas. By measuring these loads, we can assess an individual's aptitude for a particular task, their ability to perform it, and the level of difficulty they experience. If a person is trained in a completely stress-free environment, the training may not be effective. The Yerkes-Dodson Law posits that an optimal level of stress enhances performance.

Based on this comprehensive data, we initiated the 'Genius' project. Our objective was to determine whether we could differentiate the aptitude and proficiency of pilots with varying experience levels in a flight or F-16 full-mission simulator. Furthermore, we aimed to develop personalized training programs tailored to individual pilot needs. To achieve this, we

employed a suite of sensors, conducting analyses of electrocardiography, electroencephalography, and respiratory rate. By correlating these measurements with pilot performance in the simulator, we derived a set of metrics that enabled us to accurately classify pilots as instructors, trainees, or experienced personnel with an 80% accuracy rate. However, even with effective training, the question remains: what challenges will these pilots encounter within the aircraft at altitudes of 20,000, 30,000, or 50,000 feet? Traditional medical examination and analysis methods are insufficient to address this.

This need led to the development of aviation medicine, a field that originated in the 1920s. Notably, in the 1930s, Gazi Mustafa Kemal Atatürk signed a decree to send the first Turkish space physician to the United States for training, highlighting the long-standing importance of this field in our country.

A strong foundation in physics is essential in aviation science, as it allows us to understand the physiological challenges faced by pilots. We categorize these challenges into two primary groups: High Altitude Related Stressors and Mechanical Stressors. High Altitude Related Stressors encompass factors such as changes in atmospheric pressure, variations in the partial pressures of gases, and exposure to radiation. Mechanical Stressors, on the other hand, include gravity, acceleration, high-speed motion, and three-dimensional positional changes.

So, what are the consequences? In aviation medicine, we encounter three fundamental issues. The first is the loss of Spatial Awareness (SA), where an individual becomes disoriented and loses their sense of position in space. Our spatial awareness is a complex perception derived from the integration of visual cues, vestibular input from the semicircular canals in the inner ear, and proprioceptive feedback. When one of these systems malfunctions, SA is compromised, resulting in disorientation and loss of directional awareness in three-dimensional space. How prevalent is this? The United Kingdom and the United States, which maintain comprehensive reporting systems, document between 90 and 100 cases of SA loss annually. SA loss is essentially a neurological betrayal. Individuals experiencing it become disoriented, unaware of

their surroundings, and unable to process information coherently. Despite their efforts, they are unable to comprehend their actions. Hypoxia, or oxygen deprivation, occurs when the brain's oxygen requirements are not met, typically due to insufficient oxygen intake by the body. This condition is responsible for approximately 100 to 200 incidents per year. Hypoxia effectively disables the decision-making process.

Another significant challenge is the continuous variation in the magnitude and direction of the gravitational force vector, known as A-loc and G-loc. The most critical threat we face is the fluctuation in this gravitational force vector between upward and downward directions. This is due to the heart's limited capacity and pumping ability.

If you place a burden that exceeds the heart's pumping capacity, it will fail to circulate blood effectively. This can lead to a loss of consciousness, similar to an epileptic seizure. Pilots contend with a spectrum of severe effects, from visual impairment to complete unconsciousness. To address these challenges, specialized training is provided. We sought to investigate whether we could capture real-time physiological data from pilots, along with the physical forces they experience.

The project aimed to enhance pilot training in F-16 Full Mission Simulators by objectively assessing neurophysiological and physiological changes, thereby enabling personalized training programs. We achieved this at a remarkably low cost. The project proposal, initially submitted in 2013, was approved in 2017, leading to the commencement of prototype development. Our initial tests were conducted and reported in July 2020, and the final test results were documented in the same year. We successfully completed our maiden flight on November 7, 2020. What are our future plans?

What will we do in the future?

'The true essence of flight is inseparable from the human brain.'
(VIDEO): «Within the Air Force, presentations are invariably concluded with references to the flight suit and the iceberg analogy.»

I respectfully submit.

QUESTION: Are there ongoing research efforts to disrupt or enhance human decision-making processes through the use of directed energy weapons or other techniques within the context of cognitive warfare, decision-making, and electromagnetic spectrum operations?

ANSWER: The question pertains to the use of high-energy systems for human manipulation. In this context, the choice lies between employing a high-energy system or utilizing cellular technology in conjunction with advanced warfare techniques. The challenge with high-energy brain uploads is the unpredictable nature of their effects. Each exposure introduces a unique information load, potentially leading to unpredictable and ever-changing outcomes.

Is energy manipulation feasible? It's incredibly challenging and not particularly efficient. Has it been explored? Yes, it has. For instance, we have electroconvulsive therapy, a technique used for individuals with severe psychiatric conditions, sometimes in conjunction with LSD. We generate an electrical charge to address mood disorders. While it may alleviate one problem, it can introduce new ones. Manipulating a person with energy is far from simple.

Assoc. Prof. Dr. Murat ERDOĞAN
BAŞKENT UNIVERSITY

First of all, I would like to thank our Ministry of National Defence, our Secretariat defence Industry and SASAD. It has been a multidisciplinary study. Our engineers, physicians, soldiers, police officers, we could not have gathered all the elements that will form the soldier of the future if it were not for an interdisciplinary study. Many points have been adressed. Our present-day teams possess the fire power once wielded by Napoleon. Upon reviewing the burdens carried in global conflicts, it becomes evident that despite technological advancements, our soldiers' loads have actually increased. Scientific research indicates that they often carry up to 50 kilograms in their backpacks. This highlights our interdependence with technological progress. Technological advancements enable us to readily measure numerous parameters. We have access to systems that monitor everything from pulse rates and oxygen saturation levels to ground pressure and foot weight, all facilitated by smartwatches, belts, and pants. While technology has undeniably transformed our lives, its impact has not been uniformly positive. I will now outline a trajectory from the negative aspects to the positive.

Technological advancements have inadvertently led to a more sedentary lifestyle. While physical labor was once predominant, modern headquarters and command centers involve significantly less physical activity. This reduction in daily energy expenditure has contributed to the prevalence of 'the deadly quartet' – obesity, heart disease, hypertension, and diabetes – even within our armed forces. No one is immune to societal trends. While traditional tools like notebooks and pens are becoming increasingly rare, cell phones are ubiquitous. Technology has become so ingrained in our lives that it cannot be easily discarded, and one consequence is weight gain. This has implications for the battlefield. Can a soldier burdened by excess weight truly outmaneuver a nimble and agile adversary?

A study has revealed a 34% attrition rate within military services. Similar research and concerns exist across all armed forces. This widespread issue of technology-induced physical inactivity has prompted armies globally to implement physical and training reforms aimed at maintaining soldier readiness. Regular physical fitness evaluations are conducted, as our own military does, with successful candidates progressing to higher levels of service.

Anthropologists study how early humans lived and how we've changed with technological advancements. We've found that the biggest shift in human calorie consumption is due to reduced physical activity. When comparing the daily calorie needs of hunter-gatherers to modern humans, there's not much difference in basal metabolic rate. The main difference lies in the total energy expenditure from movement. We can compensate for this by incorporating more activity into our daily lives. On the battlefield, several factors impact performance: increased loads, heat, cold, altitude, hypoxic environments, climatic conditions, and muscle disorders. However, we can mitigate these effects through altitude training, acclimatization, and simulating battlefield conditions in our exercises. Updating fitness regimens to reflect combat scenarios also enhances soldier performance.

We constantly talk about energy. The energy that keeps us going is provided by a scientific substance called Adenosine Triphosphate (ATP) and it is stored in our body. We consume this very quickly. In the acquisition of energy on the battlefield, we use carbohydrates, fats and protein for this energy supply. It is important to support the soldier with scientific and technological methods in combat conditions and to inform about this in terms of awareness. There is no problem in our muscle in the first two seconds of ATP use, because it is in our muscle, as the time increases, as we come to 10 seconds, as we come to 15 seconds, our muscle store no longer allows it and we use the energy deficit from the system we call lactic acid for energy gain.

This provides us with energy for up to two minutes. Beyond this, as lactic acid levels decline, we transition to the aerobic system. Examining the impact on calorie consumption and soldiers today, scientific studies reveal that while headquarters

personnel require approximately 2700 calories, infantry and special forces, whom we consider warriors, expend nearly 5000 calories. Is prolonged engagement a disadvantage? Absolutely. Extended periods on the battlefield pose not only physiological challenges but also psychological and motivational ones. I believe that one of the valuable outcomes of this two-day event would be to holistically assess our soldiers, encompassing their physical and emotional well-being, to optimize our battlefield effectiveness. As time progresses, the body increasingly relies on fat reserves for energy, while carbohydrate utilization decreases. Energy expenditure also varies depending on the combat environment. A 40-kilogram backpack, for example, becomes increasingly burdensome, leading to diminished strength and endurance. Consequently, we must adapt our training regimens accordingly. Caloric expenditure during training is also critical. Preparing soldiers for hot-weather operations in cold environments is physiologically and psychologically detrimental. Battlefield tasks include lifting and carrying, ammunition handling, climbing, digging, walking, running, pushing, and pulling.

What are the demands placed upon us by the battlefield? We must possess tactical proficiency, marksmanship, navigational skills, and the readiness for close-quarters combat. How do we achieve these? Through the integration of mobility, strength, and endurance in our training programs. We tailor these elements to meet our specific physical requirements. While optimal nutrition and rigorous training are essential, they are rendered ineffective if the soldier lacks adequate rest. A well-balanced approach to nutrition, training, and rest is crucial to maximize physiological benefits.

When going to the TEK-ER, when training, we must personalize our trainings. Everyone has basic needs, there must be basic aerobic endurance, but for special units and special forces above a certain level, additional one-on-one trainings are essential to increase their abilities.

What physiological changes occur during combat? In the field of sports physiology, Guyton's physiology textbook, which we used in university, explains why the chapter on sports physiology is placed at the end of the book: 'During exercise and sports, the human body undergoes such a multitude of

changes that we first explain normal physiological functions, such as the heart, kidneys, and lungs, in the preceding 83 chapters, and then delve into abnormal physiological responses here.' For instance, a comparison is made between a 40-kilometer marathon runner and an infant with a 40-degree fever. While an infant's metabolic rate increases 20-fold at 40 degrees fever, it escalates to 20,000-fold during a marathon. Therefore, the physical demands of the battlefield are comparable to those of strenuous exercise. However, traditional exercise science overlooks the emotional and psychological dimensions. This is where technology becomes invaluable. By integrating technological simulations into our training environments, we can gain a more comprehensive understanding of the soldier's experience.

The physiology of combat involves significant cardiovascular changes, including alterations in venous return and increased tension. Respiratory changes occur, with compression in the chest cavity. The human body experiences immense stress as it navigates the fine line between life and death. On the battlefield, we simultaneously observe numerous physiological responses, such as changes in blood flow, density, pulse rate, and rapid, deep breathing. Advances in technology, such as MRI, could reveal a multitude of physiological stressors in any individual. By measuring these changes in real-time on the battlefield, we gain a deeper understanding of our soldiers' and officers' physiological condition. For instance, if two soldiers run 200 meters at the same intensity, and one arrives with a pulse of 160 while the other has a pulse of 140, this 20-beat difference could represent the margin between life and death. It might indicate that one soldier requires a less strenuous training regimen. We must leverage technology to scientifically enhance soldier development. Devices that monitor fatigue can help us optimize soldiers' rest and recovery periods.

We observe significant posture-related issues and challenges associated with heavy load carriage among our soldiers and police officers. These problems, potentially stemming from a lack of static and dynamic exercises or the neglect of such activities, can manifest as arm numbness due to backpack weight, and in severe cases, even lead to paralysis.

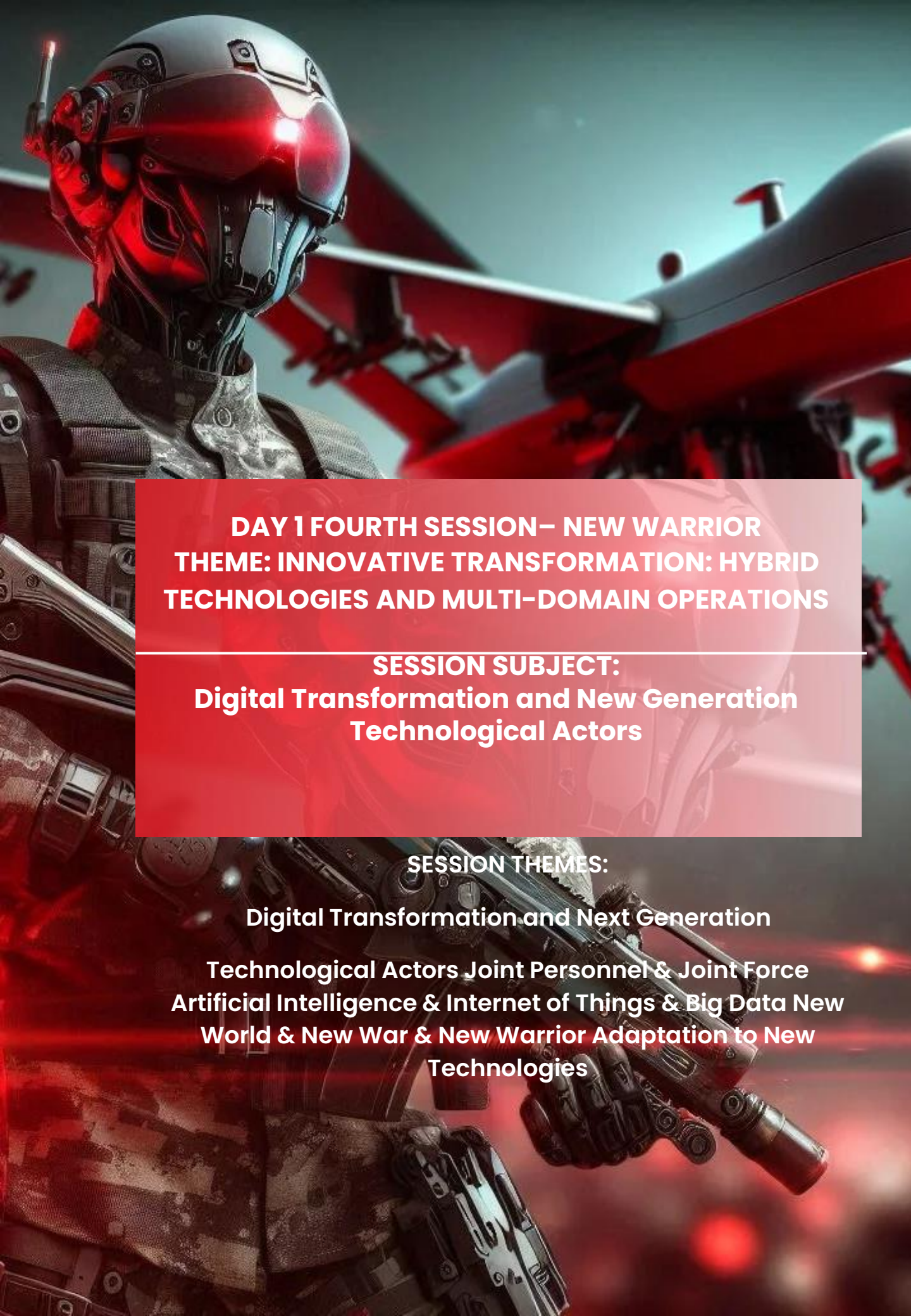
Back pain is a common ailment among our combat personnel. Even the way a backpack is loaded, the organization of its contents, plays a crucial role. We recently saw ASELSAN's load-bearing apparatus. It is imperative that we implement these technologies and translate them into practical solutions. From a physiological standpoint, we can provide soldiers with essential supplies such as energy supplements, nutritional aids, and metabolic regulators directly within their backpacks. This allows them to replenish carbohydrate deficiencies, maintain hydration, and utilize ergonomic support as needed.

The most important point is the issue of reaction speed. Today, the most important physical response that the soldier can give. Because it is no longer endurance warfare, but reaction warfare, related to reaction and developing this time, that is, we are doing physical work. The world is now working on how to improve physical reaction speed. Today, the parameters of the majority of trainings are now shifting from endurance to speed, strength and power. While endurance was more in the foreground in conventional warfare, there were many problems related to soldiers reaching and walking. Today, as transportation progresses further, it demands a balance of strength/speed and endurance to do more operative work more quickly.

Each mission has its unique set of demands. Therefore, we must tailor and manage our training and physical conditioning accordingly. During my time in the armed forces, we developed specialized training protocols for each military occupational specialty. By training across multiple tasks and energy systems, we enhance our understanding of our capabilities and improve our chances of success on the battlefield. The key is to understand our soldiers' strengths and weaknesses in relation to their mission requirements. Self-awareness is crucial for victory; it enables us to better analyze and optimize our performance.

NOTES FROM THE PRESENTATION:

- Training should be multifaceted, incorporating a range of movements like running, jumping, walking, crawling, and climbing, rather than focusing on a single task. To develop these adaptations in our soldiers, we must design a comprehensive training program that encompasses diverse combat scenarios, executing each drill with maximum intensity to simulate real combat conditions. Physical readiness is the commander's responsibility, and conditioning goals should be directly aligned with the unit's mission and its capacity to conduct full-spectrum operations.



DAY 1 FOURTH SESSION– NEW WARRIOR
THEME: INNOVATIVE TRANSFORMATION: HYBRID TECHNOLOGIES AND MULTI-DOMAIN OPERATIONS

SESSION SUBJECT:
Digital Transformation and New Generation Technological Actors

SESSION THEMES:

Digital Transformation and Next Generation

Technological Actors Joint Personnel & Joint Force Artificial Intelligence & Internet of Things & Big Data New World & New War & New Warrior Adaptation to New Technologies

FOURTH SESSION SUMMARY

Advancements in artificial intelligence will be driven by your objectives and desired outcomes, as well as those of your competitors. Examining other nations' defence spending and priorities provides valuable insights into the strategic use of AI in defence. The initial phase of AI involves machines executing pre-programmed instructions. The second phase focuses on processing and interpreting vast amounts of data. The third and most advanced phase centers on autonomous learning and application. This should be a key strategic focus for Turkey's AI roadmap. The United States and China are pursuing the integration of thousands of unmanned systems, and many countries are exploring the synergy between AI and unmanned technologies. Swarm technologies, which facilitate collaboration among diverse platforms, hold immense potential for creating significant added value.

Nations are developing AI capabilities for both offensive and defensive purposes. Offensive AI will provide an advantage if it can effectively bypass defensive tactics. For instance, the ability of a missile to prioritize targets based on their perceived threat level is considered a key advancement in new technologies. In unmanned, remotely operated systems, reliance on rigid, centralized command structures can hinder multi-domain operations. Therefore, the force-multiplying effect of defensive AI is considered a pivotal factor that will redefine roles in the application of artificial intelligence.

The development of technologies for multi-domain operations (land, air, sea, space, and cyber) is focusing on regional deployments rather than a full-scale, simultaneous battlefield application.

Dr. Poyraz Alper ÖNER
SAVUNMA SANAYİ BAŞKANLIĞI (SSB)
MODERATOR

Distinguished participants, a warm welcome to you all. I am delighted to be present at this event, organized through the initiative of SASAD, and with the valuable support of our Secretariat of defence Industries and the Ministry of National Defence. Prior to my arrival, I posed a question to an AI, using relevant keywords, to envision the soldier of the future. The most prominent characteristics highlighted were high speed, agility, and strength, with speed being the paramount attribute.

We are witnessing the integration of speed, command and control decision support systems, and wearable sensors. Where is this leading us? While we have an abundance of sensors and decision-making tools, have we considered the administrative framework necessary for their effective deployment in the field? Yes, we have. Our Operations Support Department has been established and is now operational. In our main system acquisition strategy, we are prioritizing rapid capability development through an operational support concept, taking into account the pace of technological advancement and the specific needs of the individual soldier. We are focusing on fundamental requirements.

In conducting these initiatives, we are employing an agile project management approach. Within this framework, we prioritize timely delivery over cost and performance considerations. We operate under the principle that a viable solution implemented today holds greater value than a theoretically perfect solution in the distant future. We are committed to refining our prototype-based products through iterative feedback loops. We are leveraging the capabilities of big data and artificial intelligence across all domains.

I would now like to yield the floor to our esteemed guests.

Dr. Heiko BORCHERT
DAIO
GERMANY

It's a pleasure to be here with you today. I previously worked on unmanned maritime systems for a defence company in Germany, and now my focus is on the application of artificial intelligence.

Despite the work on defence artificial intelligence, the reality is that the use of artificial intelligence by the armed forces is evolutionary. Because it is revolutionary and evolutionary, you must ask yourself this critical question. 'What should artificial intelligence do?'

'What do you want from artificial intelligence, what should it achieve?' You cannot make a comparison without knowing and determining your strategic ambition level. If you don't have a comparison, if you don't have a road map, you won't know what to follow and what to do. You cannot determine whether you are on the road.

As a culmination of extensive research, my book, 'The Very Long Game: 25 Case Studies on the Global State of defence Artificial Intelligence', presents a comparative analysis of how 25 nations define artificial intelligence. We examined a diverse range of countries, beyond just NATO and EU members, as there are numerous perspectives and initiatives surrounding artificial intelligence. How do nations perceive defence artificial intelligence, and how are they structuring their efforts? What research and priorities are driving the development of defence AI? Where are they allocating their resources, and how are they managing AI funding? It is essential to understand the six key areas of focus for nations in military AI. These include: Thinking and Concepts, Organization, Funding, Research and Development, Implementation and Deployment, and Training.

Western countries have different strategies against their strategic competitors. Get to what some western nations call their strategic challengers, how they work against their competitors, how they work against China, Iran, and what they are doing in these areas?

The term 'artificial intelligence' can be misleading. It's more accurate to think of AI as a collection of methodologies. You need to identify the most appropriate method to achieve your strategic objectives. The defence Advanced Research Projects Agency (DARPA) makes a useful distinction between three waves of AI. The first wave involves machines executing pre-programmed instructions. The second wave focuses on processing and interpreting large datasets, akin to big data. These first two waves primarily aim to improve efficiency and effectiveness. However, the third wave has the potential to be truly transformative. This wave centers on autonomous learning and application. These will be systems that comprehend their operational environment, understand the consequences of their actions, and, crucially from a military perspective, anticipate the effects of adversarial actions.

This morning, I listened attentively to the EDOK presentation, as it addressed a question we've been pondering. We are presented with a two-by-two paradox, or a two-by-two matrix that attempts to categorize 25 nations, focusing on human-centered versus technology-centered paradigms, and data-driven versus context-driven approaches. Vertically, we see a distinction between the second and third waves of AI. Horizontally, we have the human-centered paradigm, where, as the commander emphasized, humans remain central and in control. This more centralized, human-centric approach envisions machines and humans working collaboratively in teams. Alternatively, there's the third wave, where the contentious issue is whether we're prepared to fully delegate decision-making authority to machines.

Take a moment to consider: where does Turkey stand in this landscape? Where do Russia, Germany, or France fit? The intriguing observation is that all 25 nations we've analyzed are operating within the same paradigm. They are all grappling with the same fundamental challenges. This is why I emphasized earlier that the current discourse surrounding defence AI is far less revolutionary than it may seem. If every nation is confined to a data-driven, human-centric paradigm, then we should not expect any disruptive breakthroughs.

While it’s not surprising that most are within the same paradigm, some interesting contenders are poised to disrupt it, notably the United States. The US is one of the few nations actively pursuing the third wave of AI, aiming to integrate it into

their strategies. For example, through initiatives like the 'Replicator' program, they envision deploying thousands of unmanned systems, potentially in the defence of Taiwan against a Chinese incursion. Interestingly, if the US shifts towards machine-centric decision-making, China is likely to follow suit to prevent the US from gaining a significant advantage. Turkey and Ukraine are particularly intriguing in this context, as they both operate on the cutting edge. This position, while challenging, offers far greater potential than remaining within a comfort zone. Turkey now faces a critical decision: whether to maintain its current trajectory or embrace machine-centric decision-making. Concepts like 'Digital Troops' suggest a leaning towards enhancing existing systems with AI, which would keep them in the left column, albeit potentially with increased machine autonomy.

The fundamental question is whether this is purely a technological issue, or a strategic and conceptual one. Do we remain in the lower-left quadrant, or do we strive for the upper-left? Ukraine is a prime example of a nation actively pursuing this path. The lessons learned from Ukraine's conflict with Russia are evident. Ukraine's experience with remote-controlled systems highlights a critical vulnerability: the communication link between the control station and the unmanned assets. Therefore, to effectively utilize unmanned systems, increased autonomy is essential. This is also reflected in the current priorities for research, development, and application of defence AI. The use cases prioritized by most of the 25 nations we've analyzed reveal a clear trend: the integration of AI with unmanned systems, particularly for intelligence, surveillance, and reconnaissance missions. This includes AI-powered object recognition for distinguishing between civilians and combatants, enabling targeted engagements.

To understand whether deviations for use are emerging, you should not only look at the most suitable use cases, but also at the areas in which they are used, you should look at which countries are currently using artificial intelligence in which areas. Such as disaster relief, security, swimming, air traffic management, border security or close range weapon system. You see a serious difference between military uses and civilian uses or emergency uses. Because the subject is tactical.

High-scoring topics are unmanned systems, border surveillance, reconnaissance, command and control, cyber areas. Low-rate areas are areas such as border surveillance or emergencies, which can also be used in military areas. This is what Jean Marc Rickly mentioned earlier, that is, the defence meta universe comes into play at this point. This is where a few countries are currently focusing, because the surprise may be here.

We are currently developing an AI defence project for the German Ministry of defence. Based on a weapon-based system of German guard and artillery systems used in Ukraine, collaboration scenarios between different elements for a more valuable target are being studied. Currently, AI usage is being studied on a virtual twin of a battlefield with a ground resolution falling to 10 centimeters. AI imitates all the characteristics of certain assets in manned systems, physical characteristics, weather conditions, etc. And it offers us ideas or alternatives about its own attack method. Today, everyone is talking about moving in swarms. However, most swarm movement concepts are based on the rest of the swarm imitating the behavior of the swarm leader. In air systems, each has its own task, each has its own responsibility, target and mission. Now, the interesting thing is that AI teaches individuality and abandoning an individual task for the benefit of cooperation. If cooperation between different elements of the swarm means hitting a target with greater value, or if it means defending or protecting a greater value, this is what is modeled here. To bring different elements together for a bigger target.

As Jean Marc pointed out, the offensive use of artificial intelligence is likely to yield the most significant advantages. In warfare, the adversary always has the initiative. An attack will only be successful if the defender cannot effectively counter it.

We have another tactic developed for land-based defence, a system that assesses whether an incoming object is a missile.

Is nobody addressing Ukraine's most pressing challenge? The disparity between the cost of relatively inexpensive unmanned systems and the expensive missiles required to defend against them. The cost-benefit ratio of expending a million-dollar missile against a two-thousand-dollar platform is simply unsustainable.

Therefore, we are developing a tactic that teaches AI to differentiate between targets that warrant missile engagement and those that can be countered with land-based air defence systems.

There are no humans involved; it's purely machines and AI learning battlefield behavior. This is the capability offered by third-generation AI, and it defines your strategic positioning. The analysis of 25 nations reveals both expected trends and surprising divergences. For example, while it's true that wars provide valuable lessons, one must carefully interpret the observations. Many Western observers are impressed by Ukraine's use of AI for joint operations, creating a multi-source fusion picture. However, they overlook the fact that replicating this common operational picture in most EU and NATO countries is impossible due to confidentiality constraints. Data sharing between different services is restricted. Law enforcement data cannot be shared with military forces. And, crucially, within the EU, it's inconceivable that civilian iPhone data would be integrated into a common operational picture. While these practices are effective in Ukraine, they are not feasible within the EU.

A crucial point to grasp is that defence industry innovation follows a developmental trajectory, much like that of a child. This morning, I believe there was a question regarding how to optimize production capacities for legacy systems by comparing their performance with that of emerging technologies. The challenge lies in the fact that few nations excel at fostering a cohesive ecosystem that effectively integrates startups, established defence contractors, research and technology organizations, and the armed forces.

Despite their perceived strengths, all nations that excel in this area share a common challenge. Specifically, those countries considered leaders in public sector digitization often struggle to translate these advancements into tangible benefits for their armed forces.

Estonia is a leader when it comes to e-government, but the army and armed forces are very hesitant to start with new technology. Estonia is not a country that has a plan about artificial intelligence, neither is Israel. We have Israel at the point where Israel is an organized mess. Because it is in a bottom-up system rather than a top-down system. Israel does not have a

special defence-oriented artificial intelligence budget and a special defence-oriented artificial intelligence strategy. So all the elements you would normally have are not in place, everything is driven bottom-up, not with all the opportunities, but also with the risks.

TSMC in Taiwan is at the forefront of chip manufacturing, a critical component of defence AI. Unfortunately, the ecosystem relies heavily on commercial enterprises that do not prioritize defence applications. This is why I emphasize the importance of the ecosystem, which is what your question addresses. Ultimately, developing solutions that align with your specific expectations is paramount.

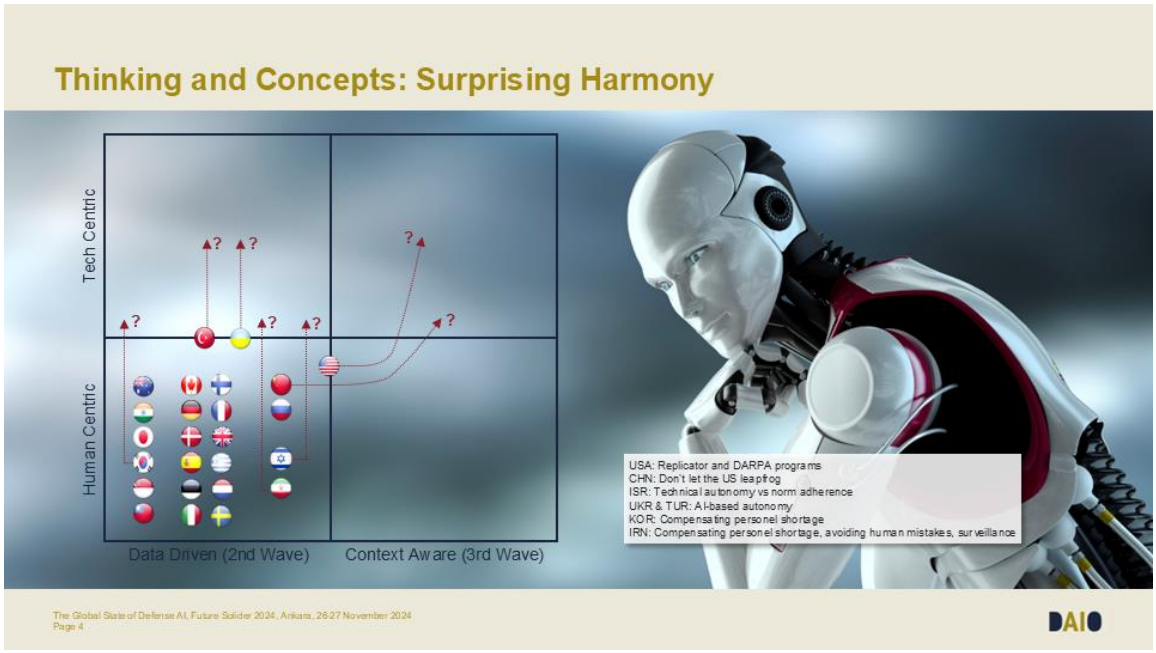
And perhaps I'd like to conclude with a slightly sobering observation. It's essential to recognize that normative preferences are being reshaped. This is evident in the cases of Ukraine and Israel. This isn't solely a technological issue. Addressing collateral damage is a human decision, not a technical one. When we examine nations currently engaged in conflict, we see that their priorities are vastly different from those focused on regulating AI in a peacetime context. It's crucial that we understand and reconcile these potentially conflicting preferences that arise from operating in peacetime versus wartime.

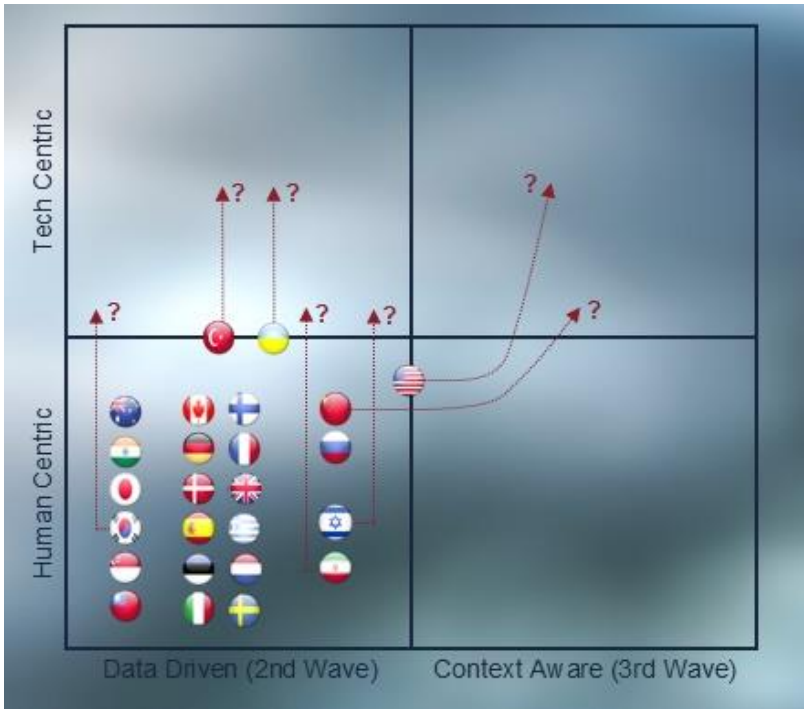
Thank you.

QUESTION: What key factors distinguish Ukraine and Turkey within the human-centric and technology-centric paradigm? In your view, what will shape the future of artificial intelligence deployment?

ANSWER: The strategic priorities set by the Ukrainian Presidential Office are clear. The priority and future lie in autonomous systems, not remote-controlled ones. This is the strategy that clearly distinguishes Ukraine. This is a possible past assumption that Turkey could take when you take into account all the different development standards. This was initiated by SSB in the last 10 to 15 years. This is not what the Plus defence industry does. Turkey has put command control unmanned systems to the fore. If you continue to adhere to a hierarchical and centralized command control in unmanned remote-controlled systems, you will never do multi-domain operations, this is really one of the key issues. Because all data sets will then come to the center and return from that center, then of course the enemy is certain. And if you have a decentralized command control center, you know that this should be eliminated first and you shoot. Then, of course, if your decentralized capabilities need to enter decentralized command control, and if this is a mentality issue, it is clear what the opponent will hit first. So, unmanned systems, command control logic, SSB priorities for the operational picture. There is a really interesting element that there are two countries that really emphasize the use of low-grade use cases to improve their defence industry's capabilities and abilities. One is Turkey and the other is Russia. If you bring these four efforts together, my comment goes in this direction. My comment is this, the question is: To what extent will decision makers feel? The relationship between master and servant. Man is the master, artificial intelligence is always the servant, but what do you want to do? Of course, you can completely change the roles. That's why I'm very sure that Ukraine is going the way I emphasized. For Turkey, time will tell and we will discuss this again when we come back in a few years...

Heiko Borchert's study on the trend of countries focusing on technology and human-centered artificial intelligence, mentioned in his speech and included in his book 'Very Long Game: 25 Case Studies on the State of Global defence Artificial Intelligence'.





Air Engineer
First Lieutenant Emrah SALAR
Ministry of National Defence

Lieutenant Emrah Salar,

I will explain to you the Air Force Information System (HvBS) system developed within the Air Force Command. Although wireless network infrastructures for the internet network have been established in educational institutions and social facilities throughout the Turkish Armed Forces (TAF), cellular communication networks cannot be used in the local area networks of the units connected to the TAF network. Wireless network infrastructures created for the internet network in training institutions and social facilities across the Turkish Armed Forces (TAF) are available, but cellular communication networks cannot be used in unit local area networks connected to the TAF network. With developing technology, the need for mobile use of information systems is increasing day by day, and there is no current capability for the use of cellular systems (4.5G-5G) in the TAF Network. In the Air Force Command, flight line personnel, maintenance personnel working at the aircraft in aircraft maintenance hangars, in training, simulator environments, glasses and equipment used in augmented reality, virtual reality applications and IOT devices depending on developing technologies are needed to be used wirelessly connected to the TAF network. In the current situation, wireless modems and similar systems can partially and locally meet the need, requiring the installation of wireless modems and/or routers wherever connection is desired, and it is assessed that their coverage areas and speeds will remain limited and low in the future. With this project, it is aimed to develop a secure wireless communication network infrastructure on the TAF Network using National software and hardware, to make the Air Force Information System (HvBS) usable with mobile devices with this infrastructure, and to disseminate this system to the units. In addition to meeting the needs of the Air Force Command, by providing secure voice and data communication with the necessary security measures taken in the TAF Network

environment using technologies such as 4.5G in the wireless environment across the TAF, with the necessary security measures taken in the TAF Network environment on ships in transit, secure. By providing secure voice and data communication with the necessary security measures taken in the TAF Network environment on ships in transit, aircraft maintenance hangars and forward operating points, the effectiveness and scope of the operation are increased and mobile capability is provided to the TAF.

In addition to benefiting from the encryption protocols found on today's wireless access devices, hardware and software encryption will be performed. Access and mobile client management function will be established, and with this capability, user authorization and system control mechanisms will be separated. Providing fast and reliable communication in military operations, supporting field operations with customized applications and services, strengthening emergency management and coordination, providing secure data transfer, data security and confidentiality by minimizing intrusion risks, cellular technology (4.5G-5G); having many advantages such as wide coverage, high data rate, high quality service and security, thus enabling location-independent, mobilized and secure use of systems, broadband infrastructure; being the basis for many technologies such as artificial intelligence, autonomous systems, augmented virtual reality, cloud computing, swarm-intelligent systems, big data processing, industry 4.0, being able to carry wireless local area network capability to the desired region via fixed base stations or mobile portable base stations that can be realized in the future with cellular network, enriching and modernizing the existing communication infrastructure usage area, Turkey's strategy "5G and Beyond" will both meet the current needs and enable the rapid introduction of 6G technology to the system and create infrastructure.

The infrastructure and capabilities to be established with the project will form the basis for the goal of "reaching a force structure that includes wireless secure communication systems".

QUESTION: Can you say something about the completion time of the project?

ANSWER: Currently, our tests continue at the Air Force Ahlatlıbel Air Radar Position Command. Our efforts also continue to do it on the TAF number 1 network. We aim to complete and disseminate the project in 2025 with the permission of our Ministry of National Defence and our General Staff.

Semih DEMİRTOKA
HAVELSAN

Hello, I am delighted to join you at this excellent event.I plan to provide an overview of hybrid technologies, followed by a high-level perspective on multi-domain operations, the NATO strategy, the Turkish strategy, and conclude with some foundational insights into products shaping the future soldier. Today's modern warfare involves several key concepts, including 'convergent interoperability and adaptability'. I would like to give examples of convergences that combine traditional and emerging technologies, such as planning AI-dependent unmanned aerial vehicles (UAVs) and independent UAVs for Dynamic Task. Planning UAVs can independently identify and prioritize targets while supporting manned attack aircraft in combat operations. Mr. Heiko mentioned a similar scenario in his presentation, but here, for example, concepts such as loyal wingman or Manned-Unmanned Teaming (MUM-T) come into play, or perhaps a land combat vehicle integrated with UAV support. As HAVELSAN, we did this, we did this in our unmanned aerial vehicles, and unmanned land vehicles can communicate with each other. I would like to give an example of swarm drone technologies within the scope of convergence. Foreigners, the US navy has a low-cost program, we also have a defence procurement agency in Turkey, there are similar programs. The example I gave you here, like the US navy, is a low-cost UAVs, swarm technology program, the collective execution of tasks by drones as a system controlled by artificial intelligence. The second feature is interoperability; ensuring seamless collaboration of different systems in land, air, sea, space and cyberspace. A coordinated air and ground attack where the UAVs I mentioned earlier are integrated with the land forces, or a use case of neutralizing the sea surveillance threat, linking the sea vessel with UAVs and satellites for persistent maritime domain awareness are other examples.

Space-based support for ground operations or cyber electromagnetic operations in air defence are also important. Multi-domain command and control is also one of the most studied topics in the United States. Many of you have heard of

the JADC2 program or initiative; this initiative basically aims to connect all military platforms to a single C2 System.

In the civilian domain, I can cite disaster relief, humanitarian assistance, and naval countermeasure applications as examples. The third critical feature is adaptability. Hybrid solutions are engineered to function effectively in both conventional and irregular warfare scenarios, thereby enhancing mission flexibility. This encompasses precision counterterrorism strikes, autonomous convoy development, naval mine countermeasures in littoral zones, guerrilla warfare in mountainous terrains, border security and anti-smuggling operations, urban riot control, and psychological operations. Under the umbrella of adaptability, relevant applications include air systems, naval systems, cyberspace and electronic warfare, and fundamentally, space. For air systems, swarm drones are a prime example. Ground systems encompass all familiar combat vehicles, and notably, exoskeletons for soldiers. My colleague Çağlar Bey provided an excellent demonstration, and I encourage everyone to visit the corridor where we are showcasing our CENGAVER demo after this session, during a break, to see it firsthand and ask questions. Exoskeletons for soldiers enhance physical strength and endurance while incorporating head-up displays for real-time situational awareness.

Mr. Heiko mentioned ethical concerns, and I would like to state first of all. The first challenge is interoperability and ensuring that the hybrid system from various nations or vendors works seamlessly together in coalition operations, which is easier said than done. Then, we need to address ethical and legal concerns, basically such as the use of autonomous weapons, civilian harm, cloud trial damage, compliance with international law, and finally cybersecurity risk. Hybrid systems, which are extremely interconnected and make them vulnerable to cyber attacks, because in the field of cyber security, they cannot attack the natural surface.

In the cyber domain, you basically enlarge the attack surface and become fundamentally more vulnerable. This is where multi-domain operations (MDO) in modern warfare come in. Multi-domain operations are the representative formative military strategy that integrates capabilities across

all operational domains, such as land, air, sea, space, and cyberspace, formative military strategy that integrates capabilities across all operational domains, such as land, air, sea, space, and cyberspace, and we all know that the aim is to create synchronized and overwhelming power against adversaries. The goal is to exploit vulnerabilities in these domains. Multi-domain operations concepts include domain convergence, decisive tempo, distributed operations, and dynamic targeting and application areas that I mentioned to you a few minutes ago. The technological enablers of MDO are artificial intelligence, data fusion and cloud computing, and interoperable systems, and the challenges of MDO complexity are interoperability, ethical and legal concerns, and we need a lot of resource intensity.

I will not read the entire presentation here, but we are all aware of the cycle. What cycle? I was born in 1975. When I was a 12-year-old teenager, in 1989 when the Berlin wall fell, young people were there and they only knew it from newspapers or the media, YouTube documentaries, but we went through that process, it was a unipolar world where the US and the West were the dominant powers and cultural dominance, hegemony, technological economic hegemony and most people my age would know Francis Fukuyama's "The End of Civilization" article and the example he gave was when Bill Gates showcased Windows 95. Famous sociologist Francis Fukuyama, if half the world's population watches the operating system showcase, then you know this is the proof of my "The End of Civilization, the West Won" article, this is indisputable, what will happen is that you will accept the terms and there will be neoliberal economic policies, free trade, more globalization, etc. There will be no physical war anymore, but today you know just a few days ago news channels or YouTube channels were talking about the possibility of a small tactical nuclear attack by Russia. Life is a cycle like physics, you know the waves. Light and sound are transmitted through waves, and like that, life is a cycle, so no matter what you do at this point, it is no longer a unipolar world, it is a multipolar world as we know it and all competitors are trying to get the best cutting-edge technology they can get.

Turkiye, as a strategic partner in NATO, also assumes important roles in technology sharing and joint defence projects. We are cooperating and trying to increase

cooperation in areas such as unmanned systems, fusion of unmanned systems, cloud-based computing, artificial intelligence in military applications, artificial intelligence in defence applications, intelligence gathering and use, electronic warfare capability, domestic technological developments. We have the maturity to implement and develop these technologies and our strategic importance, our geopolitical importance, our position is indisputable. We have made many developments in areas such as unmanned systems, manned-unmanned systems work (MUM-T systems), artificial intelligence, cloud-based computing systems, electronic warfare formation and teaming. Here, I can basically talk about what HAVELSAN does.

Not only HAVELSAN, you see TAI platforms, BAYKAR Platforms in the presentation. As HAVELSAN, we are one of Turkey's leading technology companies. We play a role in the development of new and disruptive technologies and presented the digital unity concept in 2020. Our vision is built on smart, autonomous, robotic system technologies and digital and wearable technologies you see in CENGAVER. Our command control (C5ISR) technologies are available. We participate in CWIX NATO 2024 Interoperability exercises every year. We have decision support and operational, Analysis, digital training and war preparations, autonomous and logistics support and information systems. Our products include the SANCAR platform, our armed unmanned service vehicle. This is not a picture, it's real. Likewise, CAKA is in the R&D process. CAKA is a kamikaze vehicle that can be used in submarines. It is still in the R&D process and is designed as a high-speed vehicle. This is BARKAN, BARKAN is our design privilege. I would like to state here that we are not a platform company. We are not a platform, weapon system company, we are not a hardware company, we do not produce hardware, we are a system integration company. We bring all these components together and turn them into products for the use of military authorities. And we have unmanned aerial vehicles with swarm capability. For example, BAHA, a sub-cloud system. Its big brother is BOZBEY, which is bigger. And we will add some exciting surprising features to BOZBEY. This is our quadcopter Poyraz. And also SONGAR, which is famous for its weapon rotation systems. Thank you for giving me and my institution the opportunity to express our vision on the future soldier concept.

QUESTION: Unmanned systems have started to proliferate in all areas of the armed forces. Our Armed Forces are also experiencing changes within their own structure. Is there a concept of 'Digital Units' that includes unmanned sea, air, land and human? Are field studies being conducted?

ANSWER: In all these studies, we are already progressing by collecting demands in the field together with our Ministry of National Defence and the commanders in the relevant forces, and by receiving feedback from prototype and development-oriented products before producing the final product. My opinion is that we have increased our soldiers with the technology level and increased the capability of our soldiers. We still have a way to go to the point of very autonomous platforms, completely self-moving platforms. It is being developed to help and support the soldier, our goal in the current period is like this.

DAY-1 FIFTH SESSION – NEW WORLD

THEME:

PARADOXICAL LIMITS OF TECHNOLOGY

SESSION SUBJECT:

Energy, Logistics, Intelligence, Employment and Technological Limitation

SESSION THEMES:

Qualified Personnel

Planning and Collaborations for Technological Transformation

Strategic Importance of Developments in Technologies

Mobile and Modular Operational Capabilities

FIFTH SESSION SUMMARY

Thinking outside the box and developing concepts beyond the ordinary with developing technologies will be a topic that will provide great advantages in the field of defence. An agile organization, strong people, teams that think differently and have different technological capabilities will also be a dynamic that affects success or failure in wars. Multiple alternatives will be required, such as preparing for what you do not know will happen and being ready for the unpredictable. Especially changing technologies will require transition period and new period preparations for the coordination between the new and the old. New technologies necessitate new thinking and idea environments. This requires accelerating thinking for new ways of thinking and measures by putting aside familiar ways and methods. Adapting to innovations may be difficult, especially in the human-machine harmony process.

The fact that the clothes of the soldier of the future are suitable for all kinds of chemical and biological environments, have communication systems that will not provide communication disruption, and have energy production systems for the new generation military equipment they use will affect the sense of security on the battlefield. Designs in exoskeletons can increase mobility by improving speed, agility and stability. Especially the information flow from unmanned aerial and land vehicles will be a factor that changes the situational awareness of the soldier in the field. At the same time, the need for protective equipment resistant to new generation munitions will increase. Helmet systems that will provide protection against explosive shock waves will be important. The security vulnerabilities and insecurity environment that technology may create may lead to the formation of critical failure points. This is very important for both autonomous and robotic systems and the individual security of the soldier in the field. The psychological conditions of the soldiers should also be supported with new training programs along with the developing technologies. In technological products, operability, logistics and maintenance should be determined at the design stage, functional needs, operational needs and sustainable technological and economic system preference and competition will determine.

In rapid conflict environments, being ready for operational use at any moment and continuous operational sustainability are also considered among the factors of success. Artificial intelligence will contribute to the production and field use of long-lasting products in the sector in processes such as product life, malfunction maintenance, compatible operation of equipment, and update needs.

To understand the digital world, the final reality of the digital world, the age of artificial intelligence, needs to be well understood. In fact, artificial intelligence is defined as a tool, and big data as content. The period that is predicted to shape the coming years is accepted as an age in which we have come from thinking machines to the age of machines that imitate thinking and offer solutions close to human perception. Its basis is to get accurate analyzes from big data and data.

In the target of data usage for land, sea, air, intelligence, operation or logistics purposes, there is a large headquarters, you have to manage it, you have to think about the tools that will help, you have to act by thinking that your competitors will develop it better than you. Artificial intelligence creates a great chain of opportunities and risks in the field of cyber security, in the field of cyber attack and cyber defence.

In today's world where artificial intelligence and big data are rapidly developing, changing technological infrastructures with short, medium and long-term planning, making rapid updates in terms of strategy and policy, and changing perspectives are accepted as the basis of rapid structuring. It is recommended to go to rapid structurings to be on the side that trains and develops language models in the development of artificial intelligence, knows what the threat will be and what we should do when it will be, that is, develops.

It is predicted that the era of data wars with the internet has begun, and that the era in which technologies that shape the world with the data obtained are taken as product outputs has begun with artificial intelligence, and that the periods in which artificial intelligence can make accurate decisions like a commander will be a result of the defence artificial intelligence process.

It is stated that materials such as data centers and chip systems that form the infrastructure of data centers, quantum computers will become increasingly important, and it is also

noteworthy as an important requirement to design the delicate balance between operability and security well in these processes in military technologies. It has been emphasized that the quantum encryption system will be critical in information and data flow processes and that it will be important to invest in the basic components of complex technological equipment. In addition, despite all technological requirements, attention has been drawn to the necessity of the army to work in a closed network environment until it has the infrastructure to use quantum or similar secure network systems. While it is stated that each country will basically work for its own interests in the use of technology, it is predicted that the use of artificial intelligence will reach a point where it can choose the most accurate possibility among billions of possibilities, and that the period when the decision-making point will be left to artificial intelligence may occur within 20-30 years.

Dr. Abdulkadir AVCI
Ministry of National Defence
MODERATOR

Welcome, everyone.

In this session, we will address the topics of qualified personnel, planning and collaborations for technological transformation, and the strategic importance of developments in technologies. I would like to give the floor to Ms. Karena Kyne, and she will share with us her experiences and views on the adaptation of developing technologies and armed forces personnel.

Karena KYNE
LANCASTER UNIVERSITY
ENGLAND

Thank you for your kind invitation. I've been doing philosophy for 25 years, and in the beginning, I did philosophy, just thinking about systems and ecosystems. Philosophically everything was connected, but it didn't work in the world. So about 15 years ago I started applying my philosophy. My fundamental question to learn has always been: 'How do we understand the world, what are the innovations in struggles, wars, and how can we address these questions? I collaborated with the University of Florida Special Operations unit, as well as with entities in Lancaster, England, and Canada, as part of the Lancaster, England, and Canadian Forces security program, and these partnerships continue. Currently, we are developing strategic games for soldiers with Archipelago of Design. When cultural, geographical, and environmental ecosystems become challenging, defence and security thinking requires comprehensive consideration, which is a difficult task. Teaching this is also complex. This needs to be taught and learned, but the key is understanding how to perceive the world, how information is generated, and how to share it effectively. Sharing is straightforward, and games facilitate this process. We have been talking about critical thinking or thinking outside the box or blue sky since 09:00 am this morning. My job, when I conduct our workshops with defence and security organizations, is what it means to think outside the box.

How do we do so-called critical thinking, thinking outside the box and blue sky thinking? Philosophy helps designs, introduces new things. Operational forces from US Special Forces were brought to us and we discussed with them for about 1 week what they were doing. What they wanted was to find out how to get involved in the change between technology and people in the military field, to establish close friendships, strong bonds, strong friendships and a sense of trust. For example, operational forces soldiers refused to communicate with cyber soldiers. They said that their colleagues working in the cyber field could not be called 'Soldiers'. Their defence was, 'Because they can't do what we can do, they work at the computer. And we are more agile, how can you make us work with them in the same way, classify them in the same way, that is, as 'soldiers'?

Having an agile organization requires working with strong people. There are those who are not as agile, strong and fit as you. But in new systems, technological development, team members are also needed for cyber. Tomorrow, this will be valid for other areas or systems as well. So the army is also in an identity change and is everyone ready for this change? We help them understand and 'frame' what identity, agility, unity are. We train them against internal threats, internal threats, internal ideas. I have done serious work in America on resistance to change. The US Navy was experiencing a serious problem in recruitments related to submariner recruitment. Young people were rejecting this job due to issues such as not being able to communicate with their families for a long time and staying away from social networks. That's why they had to rebrand their recruitment processes. Issues related to identity, how relationships are framed and how intimacy is framed were affecting young people's thinking. Telling them that they can communicate with their families at any time and providing the necessary technical infrastructure for this was affecting their recruitment. We also worked on similar issues in England.

The future is something that needs to be considered, and one of the most neglected things is: 'Preparing for what you don't know will happen.' That's why 'thinking about the foreseen and the unforeseen regarding the future' is an important seemingly unimportant.

The world is being reshaped by technological changes. We

talked about an official image of my presentation and the question 'Why don't people keep boats on the roofs of their houses for a tsunami?', for example, about keeping boats on roofs in a tsunami. Yes, it doesn't seem like a very effective solution, but it seems like a brilliant idea for the crowd of people waiting to be rescued on their roofs. If we are talking about decentralized technologies and ways, something needs to be done about them and think a little outside the ordinary. Thinking about understanding our relationship about humans and machines will be very important in the future. Military forces limited by hierarchy are also affected by technology, their dynamics are changing. Many things are changing around expertise and experts. And at the moment, it is impossible to promise predictability or certainty on these issues. But when it comes to defence and military, it has to be very organized and very predictable, ready for any eventuality. Especially with changing technologies, it will be necessary to do very new things between the coordination of the new and the old. How do we organize new ideas in military and defence organizations? What do we mean when we say the meaning and interdependence of the concept of the future? Seamless autonomous systems, real-time defence systems. We think we know something with our past experiences, but maybe they need to be revived and they may not make much sense in the future.

There are concerns about what certain conflicts might look like in the future and what uncertain environments such as climate change will bring. Perhaps if we had to find an idea of how to survive a flood or tsunami, it would be mandatory for all of us to draw lines in a certain way. Naturally, none of us would think of putting boats on houses with this possibility. New technologies force us to come up with out-of-the-box thoughts and ideas. For example, if the military, administrative organization structure, organizational structure, logistics and supply processes are not updated according to innovation, there is a situation where the result will no longer be meaningful if you do not change how things are renewed.

With all these new concepts, how can we think differently in real-time information, human-machine relations? For example, the reactions of operators in the case of operations with unmanned aerial vehicles. Thinking about the future or the soldier of the future is perhaps about leaving behind what we

are familiar with, putting aside the tools and methods we are familiar with and thinking about new ways of thinking and measures. Here it is important to understand how to break the boundaries caused by previous experiences, and for this, it is necessary to think about a wider and wider area.

For example, in Special Operations Forces, it is never possible to accept the expression 'failure' and for this they just have to succeed. Here, there is a situation such as doing the right thing to succeed, having to succeed. New develops the new and we continue to prepare the soldier of the future and the future war environments in psychological workshops. Serious psychological changes are needed for the transformation to take place, such as the new warrior, new systems. Seamless interoperability, harmony with real-time technologies between human and machine require innovations and new strategies. These have deep and complex meanings and cannot be handled superficially. We are shaped by what something means to us, but this does not necessarily mean that it is the best way. So basically, the soldier of the future needs to be developed and this is an unlearned situation. If we do not have critical thinking, if we do not think around the changes that are taking place, it will be difficult to implement big ideas and adapt to innovations.

Thank you for listening to me.

Prof. Dr. Svajonė BEKEŠIENĖ
General Jonas Žemaitis Military Academy of Lithuania

Thank you for your kind invitation, I am honored and happy to be among you. My presentation will be on the soldier of the future, technological limitations and requirements. Understanding the transformation of the soldier of the future is of great importance in determining the needs for the needs and requirements of tomorrow. My presentation includes short and medium term ultimate goals for the transformation of the soldier of the future in all studies in the world.

Future warrior clothing goes beyond traditional uniforms, functioning as a multifunctional second skin. Core features will consist of sensors to monitor vital signs (heart rate, body temperature, hydration levels) and environmental conditions. The uniforms regulate body temperature, providing thermal insulation in cold climates and cooling in hot conditions. It will also integrate camouflage technology that adapts to the real-time environment, such as active camouflage or infrared suppression. Advanced materials such as graphene will ensure that the garments are lightweight, breathable, and resistant to cutting, piercing, flames, and chemical materials, both in the transmission and portability of technology.

The microclimate vest is designed to maintain a soldier's optimal physiological state in extreme environments. Temperature regulation measures actively heat or cool the body using thermoelectric systems to prevent heat exhaustion or hypothermia. Advanced moisture-wicking and air-circulating systems for sweat management provide comfort to the soldier during high-intensity operations. Integrated energy systems minimize battery consumption while maintaining the continuous operation of technology-based equipment, and also include measures for energy harvesting from movement. Exoskeletons enhance soldiers' physical abilities by increasing endurance, strength and mobility.

Exoskeletons allow soldiers to carry heavier loads such as equipment and weapons with reduced fatigue and provide force augmentation.

Exoskeletons improve speed, agility, and stability, especially in rough terrain or urban environments, and increase mobility. At the same time, joint support systems reduce stress on the knees and back, preventing long-term injuries caused by repetitive physical exertion. Some exoskeletons will generate power as the soldier moves, contributing to the overall energy source.

The future warrior is connected to an advanced, secure network for seamless communication and information sharing: High-bandwidth, encrypted communication systems enable soldiers to stay connected with commanders and teammates in real-time. Data such as maps, enemy positions, and targets will be overlaid on visors or helmet displays. Soldiers will have access to live drone feeds, battlefield analysis, and mission updates via wearable or portable devices. Voice commands and intuitive controls will enable hands-free interaction with devices without disrupting combat readiness.

Future weapon systems will combine precision, power, and adaptability, with weapons featuring smart optics and AI-assisted targeting providing real-time guidance for greater accuracy and less collateral damage. Soldiers can quickly adapt weapons to different mission types, such as switching between lethal and non-lethal modes. Directed energy weapon technologies, such as lasers, will provide precision targeting without the need for traditional ammunition. It is also planned to establish mobile energy-generating vehicles and military units solely for laser firing. Weapons will include sensors that monitor environmental factors (wind, distance, altitude) to improve shooting accuracy. Future warriors will have advanced systems to protect against physical and cyber threats. Lightweight but durable materials provide ballistic protection against bullets and shrapnel without sacrificing mobility.

For Chemical, Biological, Radiological, and Nuclear (CBRN) defence: Integrated filters and sealing mechanisms within clothing and helmets will offer protection against hazardous materials.

The systems will include cyber-level encryption and firewalls to prevent hacking attempts on a soldier's communication or network-connected hardware. Protection against explosive shock waves will be embedded in armor and helmet systems as shock absorbers.

Future Soldiers' helmets will combine protection, vision enhancement, and communication technology, providing soldiers with the highest level of situational awareness. Helmets with integrated Augmented Reality (AR) systems will display real-time information such as maps, enemy positions, and team status. Advanced optics will enhance visibility in low-light or dark conditions, with night vision and thermal imaging methods increasing mobility at night. Microphones, speakers, and noise cancellation systems will ensure clear communication in loud environments, while helmets providing superior protection against bullets, shrapnel, and blunt force trauma will be indispensable. Environmental sensitivity sensors will detect chemical or radiation threats and instantly warn the soldier. Power systems for future warriors are designed to sustain all high-tech equipment without adding excessive weight. High-capacity, lightweight batteries will provide extended operation for wearable technology, exoskeletons, and weapons. Devices will harvest and store energy from the soldier's movement (e.g., kinetic energy) or environmental sources (e.g., solar panels). Portable charging systems or base stations will allow soldiers to recharge equipment in the field. Intelligent systems offering efficient power management will ensure uninterrupted operation by prioritizing power distribution to critical devices.

Studies focused on optimizing the physical, mental, and cognitive abilities of soldiers are quite common in the future soldier concept. In cognitive development, brain-computer interfaces (BCI) and neural stimulation will enhance decision-making, focus, and situational awareness.

Sensors will monitor stress levels and provide real-time interventions, such as guided breathing exercises, to maintain composure in high-pressure scenarios. Intelligent systems will track a soldier's energy needs and offer tailored recommendations for nutrition and hydration.

Psychological support systems will provide mental resilience support to prevent burnout, post-traumatic stress disorder (PTSD), and other mental health issues, and the need for these programs will increase. For all these technological situational awareness and intensive technological environments, virtual reality (VR) and AI-driven simulators will allow soldiers to get used to realistic training environments and be prepared for complex tasks.

Technological advancements in precision, communication, and intelligence are transforming the landscape of warfare. The challenges encountered arise from technical, operational, ethical, and strategic considerations, highlighting the critical role of human adaptability in conjunction with technology.

Operational vulnerabilities also involve risks in a technology-intensive environment. A sensitive environment is created against cyber attacks, jams, and disruptions. Overconfidence creates critical failure points. Cost and sustainability increase high development and maintenance costs. Budget constraints for small countries are also a risk factor for the balance of power. In the future soldier concept, the absence of contextual understanding and ethical reasoning by artificial intelligence creates a gap. Complex scenarios still require human judgment. Ethical dilemmas also come to the fore as ethical accountability and concerns about autonomous weapons, as well as concerns about global acceptance and regulation. Low-cost tactics challenge advanced systems, and asymmetric threats such as guerrilla warfare gain even more power with developing technologies. This is an important indicator of the high level of adaptation of the enemy to new technologies.

On the other hand, harsh weather conditions, terrains, and electromagnetic and cyber interventions are noteworthy as the biggest environmental constraint effect of unmanned systems. Increasing trust, information overload, and decision fatigue are the biggest technological paradoxes of the 'future soldier' concept. Technological gaps and global inequalities arising from the expansion of inequalities in military power increase instability in the regions.

The future soldier concept also requires changes in the foundation of army readiness. In new technology concepts, the question 'what is ready?' should be answered with flexibility, individual and collective team training, and the ability to fulfill the tasks given through leadership.

The question 'What is resilience?' should be considered in the light of technological developments: facing and coping with difficulties, adapting to change, recovering, learning from mistakes and setbacks, and reviewing mental, physical, emotional and behavioral skills development programs.

Based on decades of operational experience and the lessons learned, the "ready and resilient" initiative outlines a comprehensive strategy designed to enhance soldier resilience through several fundamental elements:

The Whole Person Concept: The whole person approach, which recognizes the interdependence of physical, mental, emotional, and social health, emphasizes the development of resilience in all dimensions of an individual's life. This comprehensive perspective ensures that soldiers are equipped with the resources they need to be ready in diverse and challenging situations.

Training and Education: The development of resilience is integrated into soldiers' training programs, offering structured education in resilience techniques. Through the application of evidence-based methods, soldiers acquire the skills to enhance their cognitive, emotional, and physical capabilities, thereby improving their ability to adapt and excel in stressful environments.

Integrated Approach: By weaving resilience into the fabric of military life, this initiative merges individual training with unit-level programs, cultivating a unified, mission-oriented community. Embedding resilience principles throughout the organization establishes a continuous framework of support and readiness, promoting soldiers' well-being both on and off duty.

In military analyses conducted in Ukraine and Lithuania, we saw that it is crucia l for military organizations to incorporate

resilience development into routine military training to strengthen emotional, cognitive, and physical strength through integrated training programs.

It was also determined that encouraging leaders to model and promote resilience is of great value in promoting a culture of adaptability and support. Within the scope of holistic support systems, we also determined that providing resources for mental health, family support and community involvement to maintain the well-being of soldiers beyond their technical roles is also encouraging. Such motivations will be of great importance in human-technology harmony. Similarly, we determined that maintaining an optimistic and hopeful outlook that helps increase morale and motivation in challenging situations in the basic components of soldiers at the individual level, the ability to constructively manage stress and distress using healthy strategies such as problem solving and emotional regulation, helping others and developing a sense of purpose and connection that strengthens social bonds and personal well-being makes the soldier feel comfortable in teamwork. And their levels of importance are in this order.

We have found that a soldier never feels alone and feels like he belongs to a team within a team. Similarly, we have found that open, honest and effective communication in an environment they see as family promotes understanding, conflict resolution and emotional support, helps individuals maintain focus and resilience in difficult times and provides emotional reassurance. We have found that flexible and adaptable family dynamics contribute to their ability to adapt to changes such as deployment, relocation and stressors.

In summary, what I want to say on this subject is that the geopolitical situation has forced and is forcing us to have an army with the best train, that is, transportation and logistics, equipment and resources. The challenges in the world necessitate our soldiers to be the most accurate, most resilient force going forward. Therefore, we must be committed to investing in our soldiers, civilians, units and families within the scope of changing and developing technologies.

Best Regards.

Özgür ÖZDEMİR
SECRETARIAT OF defence INDUSTRIES (SSB)

Hello, my presentation will be on Total Life Cycle Cost and Logistics Support (TLCCLS) activities and predictive maintenance with artificial intelligence. The focus for the last 20 years, both in the world and in Turkey, has been to equip our army, the Armed Forces, starting from a soldier, with new weapons and systems at every level, from team, brigade to division. We have an iceberg model here. This is a good and short method for this topic.

Whether it's purchasing, developing, or procuring off-the-shelf, it all forms the top of the iceberg, but it doesn't end just by equipping a device system, a soldier, or acquiring a radar tank. For their survival, training and education needs cost, special test equipment cost, repair-spare parts cost, labor and personnel cost, supply support cost, decommissioning cost, technical data cost, facility cost, packaging, handling, storage and transportation cost, procurement and ownership costs, integrated support elements costs also need to be considered, all need to be provided. World Wars especially revealed these results. One of the elements that win wars is technological superiority, one is production capacity, one is tactical superiority, and one is logistical support, in today's terms, life cycle management. That is, the devices, systems, weapons it equips are constantly up, ready and usable. Therefore, if the top side is the procurement cost, the bottom side is the ownership cost and the total is the total cost of ownership.

If you only care about ownership and having it in your hands, these can create problems that cannot be solved with money alone. You might say you can fix some of it with money, but you can't solve it all with money. If your armies, devices, equipment, hardware, outposts cannot perform their correct duties, it can eventually lead to a survival problem, a problem of being excluded from the operation. These are the components of a whole staying alive. Now we see the importance of these, even though equipment and technology always come to the fore here, we see that the USA keeps this

data more accurately, this data exists across NATO and in NATO countries. Procurement constitutes 20 or 30 percent of your total cost, from the idea stage of the business, including design development, to the end of the initial production process, that is, until the goods, devices, systems, products reach your hands.

However, the main part of the business is the ongoing operating maintenance cost until that device, that platform, that tank is removed from your inventory and goes to scrap, is donated and granted somewhere. And there is also a decommissioning cost. When you plan this part of the business, it is 70-72 percent in the USA. If you do not plan this correctly, you can try to maintain a material you bought for one. Which happens in our country and other countries.

Another issue is that, in order to keep this entire system running, you need to make decisions during the design phase to minimize your costs, the costs of that maintenance, operation, and usage support phase, which constitutes a large part of the cost. And 85% of the decisions affecting these costs are made by the end of the critical design phase. That is, when production starts, when inventory acquisition is concerned, you have made 95% of the decisions. So, in fact, you have designed your tank, your plane, your helicopter, your ship in a way that it will be maintained. You cannot intervene in other matters that will govern maintenance, logistics management from now on. Because your design is complete and the product has emerged. If you want to be effective in logistics support and maintenance issues in this process, reduce costs, make these easier, your decisions must intervene in the process, and in our armed forces, our logistics support-related maintenance departments, or today, the product loss in our companies, integrated logistics loss, logistics units need to intervene early in the process so that when designing, not only functional requirements but also functional needs, operational needs, that is, the operation of the vehicle device, on the one hand, if this is an armed forces vehicle, its mission-related functions such as hitting what it shoots, details related to maintenance support should also be decided. Because these will govern the majority of the money you spend on this device, this equipment in the future, when you use this device. Therefore, while these decisions are made in the process up to production, those responsible for logistics support and maintenance, such as SSB

in procurement authorities, us, in the armed forces, law enforcement forces and companies, should also be at the table.

Furthermore, we are actively involved in NATO's AC 327 life cycle management programs. Across NATO member states, particularly in Western nations, allied perspectives and assessments on this matter are considered. Acquiring a device, system, or piece of equipment—be it an aircraft, tank, helicopter, or vessel—entails more than just the initial purchase. What constitutes meeting the needs? Meeting the needs signifies that the defence and security system can operate at the desired performance level with minimal cost and successfully fulfill its mission for 30-40 years, which is the duration it remains in your inventory. Therefore, fulfilling the need occurs when these criteria are met, not simply when a tank is replaced or a ship is launched. Consequently, to maintain operational readiness, you must consider factors such as usability, reliability, and mission readiness.

When acquiring any platform or system, it's essential to ensure its supportability and sustainability, and to do so within a budgetable cost. Beyond merely addressing technical specifications and performance during procurement, meticulous planning and preparation of all field-based elements, known as integrated support elements, are crucial. When all these aspects are harmonized, the needs of our armed and security forces are effectively met. Within NATO, the tank and aircraft are commonly referred to as 'focus systems,' but they are, in fact, integral components of a comprehensive process. The AC 327 process can be viewed as a tailored adaptation of this framework to suit our nation's specific requirements.

In 2017, we established the Turkish defence Industry Life Cycle Management Platform (TSSÖDYP) as SSB to promote and support these initiatives in Turkey, and to assist our entire sector, including armed forces, police, gendarmerie, coast guard, and our collaborating integrators, contractors, and subcontractors. This platform was initiated as a project in 2017 to develop solutions tailored to our national context. Similarly, NATO's initiative was established and planned for this very purpose in 2017. The objective is to establish the Life Cycle

Management Platform with the active participation of domestic contractors, users/authorities, and all pertinent stakeholders, implementing the Life Cycle Management (LCM) approach in our projects. Our goal is to promote LCM principles and practices, which integrate procurement with usage and logistics support, and to develop nationally relevant and customized solutions for life cycle management, product support, and related aspects in defence and security programs and projects.

The organization is structured around four working groups: System Life Cycle Management (LCM), LCM and Logistics Analysis, Life Cycle and Logistics Costs, and Specialty Engineering. The working groups responsible for System Life Cycle Management and LCM and Logistics Analysis have concluded their research and released their reports. Working Group 3, focusing on Life Cycle and Costs, is in the establishment phase. Currently, Working Group 4 is conducting studies on Reliability, Availability, Maintainability, Safety, Software, and Testability. A total of 16 documents have been published by Working Groups 1 and 2. All these processes are accessible through the Secretariat of defence Industries's website.

Where technology develops, artificial intelligence is also considered in terms of maintenance, administration, logistics. We also talk about planned and unplanned maintenance. On the other hand, Predictive Maintenance is now in question in the maintenance processes of the products supplied. This was made possible by the point that artificial intelligence and technology brought us. What is predictive maintenance? It is the type of maintenance that is carried out to predict or prevent the risk of failure with the data obtained before the machine or equipment fails. That is, we prepare and operate integrated logistics support plans and maintenance plans for planned maintenance that we practice with human power. On the other hand, we also have a plan for how to intervene for the unplanned failure or post-operation situation that happens to us. We realize these when they happen to us or when we plan. Can we intervene before a failure occurs, this is the issue. Our aim is to detect failures in advance, to find them before planned or unplanned maintenance. To reduce maintenance costs, to extend equipment life, to increase productivity and efficiency in the industry. To increase the operational usage

rate and uninterrupted operation time of military platform systems. To be able to use any equipment you want at any time. How can we articulate this concept? Currently, predictive maintenance entails identifying the condition of equipment and devices by assessing pre-failure conditions through collected data and subsequently predicting maintenance requirements.

In a motor, hydraulic system, mechanical system, electronic component, temperature can be monitored, vibration can be monitored, an acoustic sound sensor can indicate a problem. You will control these through sensors and make decisions by analysing those data. The technologies that make this possible are artificial intelligence. We are trying to predict equipment status and identify possible failures by utilizing artificial intelligence and big data analysis. Artificial intelligence does this through the processes of learning from data in machine learning and collecting and sharing data by connecting devices. Data analysis enables the comparison of the current situation by following the real situation live and comparing it with past data, and the detection of abnormality. The Internet of Things (IoT) makes this possible.

Currently, we utilize 'narrow' or 'weak' artificial intelligence (AI), which is limited to specific tasks such as facial and vehicle recognition for law enforcement. These systems operate through learning. In contrast, 'Artificial General AI' represents a more advanced form of AI, designed to learn, think, and perform at a human-like level. While narrow AI is predominantly used today, Artificial General AI is still in development. Projections indicate that by 2025, 'Artificial Super Intelligence'—a third tier of AI surpassing human cognitive capabilities—will emerge, according to IBM's classifications. Another category is 'Reactive Machine AI,' which can respond to external stimuli in real-time but lacks the ability to form future-oriented memories or store information. The next stage is 'Limited Memory AI,' capable of storing information for learning and future task training. 'Theory of Mind AI' represents a further advancement, enabling the perception and response to human emotions, as well as the execution of tasks performed by limited memory machines. This AI can engage in interactive communication. The ultimate stage is 'Self-Aware AI,' which possesses self-awareness, the ability to recognize others' emotions, and human-level intelligence. Essentially, the goal is to create a

virtual human. These represent future AI objectives and classifications. As these technologies evolve, the scope of their capabilities will expand significantly.

Through machine learning, supervised learning enables model training with failure history data, while unsupervised learning facilitates data analysis and anomaly discovery. Deep Learning can be utilized to analyse complex datasets more profoundly, enabling fault detection across various data types, such as image data and audio alerts. If we monitor a system with sensors, we will have continuously updated data. Data mining becomes possible by detecting anomalies through the discovery of patterns in large data sets with live tracking. Predictive Maintenance constitutes the entirety and integration of these systems. To achieve this, we must collect data. Sensors on military vehicles, aircraft, and other equipment will gather data such as temperature, vibration, and pressure through the Internet of Things (IoT) and sensors.

Furthermore, we will analyse these through data processing and analysis, artificial intelligence, and machine learning. Ultimately, we will perform fault prediction and issue warnings. Our main objective is to enable fault prediction using past data and learned models via artificial intelligence, and to provide early warnings to maintenance teams. Solutions before failures and issues arise. When sensors, data, systems, and devices are monitored comprehensively, where do you arrive? You create a digital twin of that system, which has been done in aviation for aircraft for some time. In this way, you perform live tracking of that system and reach an advanced point.

When artificial intelligence and machine learning carry out these tasks, decision trees will be used to classify data and predict failure conditions. Support Vector Machines (SVMs) will be employed to logically classify data, providing clear predictions for potential failures. Artificial Neural Networks (ANNs) will process more complex and larger datasets, generating failure detection and predictions. Time Series Analysis will detect potential future failures by making predictions on data that changes over time. Machine learning and artificial intelligence utilize these techniques. How can we utilize these in the defence industry? The aviation sector, in particular, has been employing these for years; the F-35 is a prime example. America equips it with sensors and information to possess comprehensive operational, structural, and

situational awareness, facilitating this data flow.

We can also use this to predict maintenance for critical vehicles such as armored vehicles, helicopters, fighter jets, UAVs, and ships. Simultaneously, we can employ it to ensure the continuous operability of electronic systems like radar systems and communication equipment. We can use it to ensure the continuous operability of systems that need to function 24/7, like our eyes and ears, preventing us from being blind or experiencing interruptions. Similarly, we can use it to ensure that weapon systems operate accurately and reliably.

When carrying out these activities, what should we pay attention to when performing predictive maintenance? This is not something that can be done immediately. We need to know the mechanism of deterioration and wear, whether it is a platform, system, vehicle, device, whatever we are going to monitor, wear, damage, deterioration can occur, mechanical, electronic, chemical, so that we can model it and interpret the data we receive. You cannot set out without knowing this. After solving the mechanism, I need to know what I can monitor with and how to measure what. If I know how to measure what, I can do this monitoring. On the other hand, in order to do this monitoring, which will be through sensors and measurement, I need to store this data and constantly compare the old with the new. I should always be aware of how the situation is going, of the situational awareness. If we are entering this predictive maintenance activity, you must predict the remaining life of the parts until a functional failure occurs in themselves. If your prediction is not a prediction that you have done through people until today, as it has been until today, if you are going to do it on the planned date, it has no meaning. Or a failure occurred and you could not predict it, it has no meaning either. This makes the system fail itself. These need to be done before they fail in order for the system to work. We must catch this. While doing this, we must not forget this. We will not do this in a factory with an engineer's dream. Yes, it will start in the factory, but our vehicles, weapons, tanks, planes will not stand still in the warehouse, base, hangar. These will see the field. We will not forget the effects of the environment in which they are used, where the helicopter and plane fly, where the ship is located, even the normal effects.

Furthermore, you need to be aware of the environmental conditions' impact, which is always crucial in the military and

defence industry. You must know that a result is normal when a device goes to -25 degrees and its normal reaction effects at +20 degrees. You should not think that it is an abnormality by being affected by the conditions.

What are the advantages of this? Early fault detection: potential faults will be detected at an early stage. If you can do this, on the other hand, if you can intervene early, if it does not lead to unexpected faults, costs will decrease. We will prevent it from going to crash, failing, and major damage happening to us. This means that something we foresee today, a planned 50 thousand hours of operation, can fail in 10 thousand hours. Or a 10 thousand hour forecast can materialize in 50 thousand hours. Early and unnecessary intervention, changing the equipment 5 times or operating it for 50 thousand hours when it is working efficiently. It will prevent all unnecessary expenses.

Most importantly, the increase in uninterrupted operation, operational readiness, is the most important issue for our armed forces. Since you can perform continuous maintenance with early detection, it will increase the readiness for operation at any time. Since you ensure that the equipment does not fail, it will ensure that the operations are uninterrupted. It will also provide increased security. It will ensure that military equipment operates more safely, and will prepare the ground for our soldiers and personnel to work in a safer environment. In addition, this process will bring increased efficiency. Unnecessary maintenance activities will be eliminated, operating time will increase, operational efficiency and continuous operation will increase. These are the advantages that this system will bring.

Now, let's look at it from the opposite perspective. What are the challenges of AI-Based Predictive Maintenance? Yes, first of all, high cost. Technology is good, using it is a good thing. If you want to equip a device or equipment with artificial intelligence, machine learning, state-of-the-art sensors, if you want to equip and monitor a ship with these, you may encounter high costs. These have a cost. Is it more economical to do it, or not to do it?

On the other hand, data security. This is the defence industry, the security we are talking about. You will start collecting data, data security is important in every field, but data security of all kinds of equipment in the defence industry is more critical. Therefore, it must be protected against cyber

attacks. Data quality, since the platforms discussed are military the accuracy of sensor data can sometimes cause problems during operational use in harsh military conditions.

There are also algorithmic challenges. You will start with an existing artificial intelligence. That artificial intelligence will correlate data, learn, compare, but it will also become outdated as time progresses.

If you cannot update according to the conditions of the future and the developing technologies, accurate predictions will become difficult or unhealthy with old data. Data will accumulate, new sensors will be formed, data with higher quality attachments will come. But artificial intelligence will be outdated. Therefore, algorithms will need to be up-to-date in order to give data predictions and healthy results.

There will also be integration problems. This is one of the issues that we can all experience today. Depending on the situation we have, there is existing data. It was kept on paper, in units, in companies. How will these be put into the system? How will we do this and how will we add it to the system if we want to equip an aircraft, radar, tank that we have taken into existing inventory and that is not designed like this with these sensors? Because these were not included in its design, how will we do this without damaging the current operation?

It will also be a problem how to compare the old data presented by digital or non-digital methods that we have for the data that the system will evaluate, with the data that digital sensors and new technologies will provide.

The main issue is still humans. When we live with these systems, the education and adaptation process of people will also be a challenge. Because people will also need to be trained according to this infrastructure in the use of these technologies, and people will also need to adapt to this, personnel should also be aware.

What do we have and what can we have in the future? While constructing this, we may not see it, but autonomous, fully robotic systems will emerge. We know that we can do these even now with artificial intelligence and machine learning. In the future, perhaps machines will be able to do this on their own, they will be able to repair themselves. There are those who watch movies and see scenarios. For example, in the

I, Robot movie, there were tiny nanites. If it is thought how tiny robots, simple robots, can be given to the human body, vein, and genetically repair the human, environments where the equipment around can repair itself are considered. Therefore, perhaps this will happen in the future.

In the future, perhaps machines will be able to do this on their own, they will be able to repair themselves. There are those who watch movies and see scenarios. For example, in the I, Robot movie, there were tiny nanites. If it is thought how tiny robots, simple robots, can be given to the human body, vein, and genetically repair the human, environments where the equipment around can repair itself are considered. Therefore, perhaps this will happen in the future.

5G and 6G are on the way, IoT integration will increase, data transmission speed will increase and data tracking will become easier. Therefore, faster data transmission and greater integration of IoT devices will make Predictive Maintenance more effective. It will become easier. As a result, all systems are going to the world.

Military systems will also evolve, and although it is difficult due to security being paramount, all military equipment will communicate with each other. If you have deployed your units to certain parts of the globe, such as the USA and Turkiye, you will want to monitor and track all of them. A global data system, an ecosystem, will be formed. You will make all devices communicate with each other through data flow with satellites. The USA can do this with Starlink or its military satellites. All kinds of information can be brought and taken to every part of the world, and this will further progress. All these, while technology is going somewhere, humans also think the opposite of this situation

Industry 5.0 is on the horizon. With 4.0, we saw dark factories; with 5.0, the aim is to transition to a production model where humans and technology coexist. Because technology pushes humans aside, leaves them on the sidelines, makes them unemployed, it also has negative aspects. Hopefully, an environment where technology and humans work together, using human skills, is desired to be modeled. Let's see if artificial intelligence or technologies will make humans unemployed or if a harmonious collaboration can be achieved.

This subject is extensive. It doesn't end with these points. If these topics are to be discussed nationally within Turkiye, we have our own subjects to address. When multiple allies and countries come together within the NATO framework, the topic becomes even more profound. Different countries, different platforms, different systems will come together, and allied systems will be used. Joint operations and missions will be carried out, systems and soldiers will come from different countries, and these need to be studied. For example, what are these? What are the security risks of artificial intelligence and predictive maintenance? When you start entering data, the weakness, sensitivity, gap, or deficiency of an equipment in the field against the opposing element, the enemy element, can be detected live. This sensitive data and information will need to be transmitted preciously, not transmitted to the opponent, not go outside. This will always be a sensitive issue in military activities. We have systems in use, when there is progress with our allies or internally on these issues, how will an integration be made, how easy or difficult will it be? How it should be when you want to manage existing systems will be studied. There are commercial applications in Predictive Maintenance examples, applications in institutions such as Siemens, BMW, it is not specific to the defence industry.

If we implement these, we will ensure increased efficiency, reduced costs, operational continuity, increased operational readiness rate of devices, and long-term use. So, should a cost-benefit analysis of implementing these be performed? Equip a ship with sensors, calculate costs with planned maintenance, unplanned failure, time cost effectiveness. Which is more beneficial? What is the cost and time efficiency? In summary, is it worth doing? This also needs to be understood. Technology is good, but it may be meaningless if the results do not make much difference. There is also data related to military platforms and systems, data from users in needs authorities such as our armed forces, police, gendarmerie, coast guard, users, shipyards we call maintenance authorities, military factories. There is data from the manufacturer of this information or that tank, plane, platform, radar, armored vehicle, missile system. If a ship is equipped, there is separate data for the ship and the equipment placed on it. How will this information be handled? There are sensitivities such as commercial privacy, confidentiality.

On the other hand, when it comes to data, the reliability and accessibility of data are sensitive issues and how should they be handled? This should be discussed. What will the data structure be? You will collect data and manage it. What is healthy data, what is faulty? You are receiving data with sensors, but if the data itself is also faulty, it will deliver faulty data to you as well. The accuracy rate and value will always be important. When all these data issues come up, when they are discussed in international organizations such as NATO, regulations regarding data. How will our national data, the USA, NATO, export control mechanisms, and data received and sold from abroad be handled? How will they be mutually regulated, these are very important. The most important item is whether it is worth doing this, cost and benefit analysis. There may also be damages and threats, and all of these are open issues.

To give an example, let's consider a study from America. There is a company called C3 that works on maintenance of America's own military aircraft. 1 Chris Byrne has an analysis on this subject. America has 5,400 air platforms and is spread across nearly 200 bases. A global operation is being carried out. According to what he mentioned, they say that after a 24-week result, they achieved 6 percent efficiency in mission capacity and 40 percent efficiency in unplanned maintenance scheduling. The USA is currently using this artificial intelligence software for its air platforms all over the world. Here is a good example for our defence industry as well.

Thank You.

QUESTION: Hello, as you mentioned, the logistics support perspective is a discipline that covers a process from conceptual design to the end of the product's life, and in fact, there should be no phase difference between it and the design groups in the conceptual design section. Because when the product is delivered to the customer, its correction, the design groups will somehow be distributed, the maintenance of the product will pass to the logistics part and correcting the failures that may occur in the product during use can be expensive or impossible. With this perspective, can you share your views on logistics support analysis? Before taking your time, I would like to share an experience about the A400M aircraft. A crack occurred in the aileron fittings of the A400M aircraft. In order to retrofit this, you have to disassemble 350 blind rivets, 350 bolt nut combinations. So what is the situation in 380, it can be solved with 4 bolts in 380. This is where the importance of logistics support begins. If you miss this, you have to make a free replacement and your labor is wasted. Therefore, logistics analysis should be imposed as a must-have point in contracts, especially in the Secretariat of defence Industries

ANSWER: Thank you. With the Turkish defence Industry Life Cycle Management Platform we presented in the presentation, we established this system in 2017 with all sector stakeholders, our companies, our major integrators, our friends from the armed forces, air, land, sea, coast guard, and we took into account the perspective you mentioned. In the sector, we take into account the entirety of logistics support, namely life cycle management in general, in the activities carried out by the defence Industry Agency and the Ministry of National Defence. Everyone related to this should be in the preliminary stage of the project, in the initial stage, and they should also say what they want when decisions affecting the design are made. In terms of both task and quality, on-site maintenance administration logistics support can be very burdensome, difficult, requiring withdrawal from the front, creating results that make you pay meaningless costs. We also expect your participation on every platform, we want this to come to the fore, not to be forgotten. When this is forgotten, there is no remedy, results should not turn into a team running like 'firefighters' when there is a fire, with an example from our own culture that seems very small. We must intervene at the very beginning so that the equipment is designed correctly, is easily intervenable, and is important to be easily intervenable on the

front in case of failure or repairable in the factory. This will reduce costs. This will always increase its readiness for use rate. We also express this in every environment. This is the duty of our unit and we are working for it.

As much as we say from here, also due to the development necessity in Turkey, it is said that the demand should arise from the public or the public should own it, people from within the sector like you, people from the industry, production, design side in our defence industry companies should also express this, so that the needs authority, land, air, sea, police, security, coast guard, regardless, also the procurement authority, the defence Industry Agency and the Ministry of National defence, also the entirety of the system responsible for this, those in the project development and procurement process should also hear this voice. Thus, precautions can be taken from the very beginning. It should also come from the armed forces themselves, so that this sensitivity should not be crushed at the point of contract, performance requirements in the contract, system requirements, correct calendar, not getting into penalty and receiving payments on time.

DAY-2 FIRST SESSION – NEW WARRIOR

THEME:

STRATEGIC COMMAND AND DIGITAL COMMANDER

SESSION SUBJECT:

Energy, Logistics, Intelligence, Employment, and Technological Frontiers

SESSION THEMES:

Operational Capability

Digital Headquarters (Intelligence and Analysis)

Operation Center

Pre-operational - post-operational, addressable data

Focused and analytical data analysis

Capability/capacity expansion

Information sharing

The return of data power

Process management in remediation

SIXTH SESSION SUMMARY

To comprehend the digital world, a thorough understanding of the artificial intelligence era, the latest reality of the digital landscape, is essential. In essence, artificial intelligence is defined as the tool, while big data serves as the content. The period projected to shape the coming years is acknowledged as an era where we have transitioned from machines capable of thinking to machines that emulate thinking, providing solutions that approximate human perception. Its foundation lies in big data and extracting accurate analyses from that data.

With the objective of utilizing data for land, sea, air, intelligence, operational, or logistical purposes, you are faced with managing a vast headquarters. You must consider the tools that will assist you, while also operating under the assumption that your competitors will develop them better than you. Artificial intelligence creates a significant chain of opportunities and risks in cybersecurity, encompassing both cyber-attack and cyber-defence domains.

In today's era of rapidly advancing artificial intelligence and big data, the foundation for rapid structuring is considered to be the transformation of technological infrastructures through short, medium, and long-term planning, swift updates in strategy and policy, and the alteration of perspectives.

In the development of defence artificial intelligence, it is recommended to pursue rapid structuring to be on the developing side, which involves training and enhancing language models, knowing what the threat will be and what we need to do when it occurs.

It is anticipated that the era of data wars began with the internet, where technologies that shape the world are produced as outputs from the obtained data, and that this era has commenced with artificial intelligence. It is also foreseen that the periods in which artificial intelligence can make accurate decisions like a commander will be a result of the defence artificial intelligence process.

It is stated that materials such as data centers and the chip systems constituting their infrastructure, as well as quantum

SIXTH SESSION SUMMARY

computers, will increasingly gain importance. It is also noted that the delicate balance between functionality and security in military technologies should be well-designed in these processes as an important requirement. It is emphasized that quantum encryption systems will also play a critical role in information and data flow processes, and that investing in the core components of complex technological equipment will be important.

Furthermore, it has been emphasized that despite all technological requirements, the military must operate in a closed network environment until it has the infrastructure to use quantum or similar secure network systems. While it is fundamentally stated that each country will work towards its own interests in the use of technology, it is predicted that the period in which the use of artificial intelligence will reach a point where it can select the most accurate possibility from billions of possibilities and the decision-making point will be left to artificial intelligence may occur within 20-30 years.

It is recommended that when producing all kinds of technology, military symbology should be in a common language, and international standards should also be considered with an export perspective. It has been suggested that being within international and national communities during the technology development stages, being alongside the developers to be on the developing side, will be beneficial, and that collaborations should be developed. It is noted that the benefit and risk analyses of the models should be well-conducted as the basis for modifying, developing, and differentiating, and that roadmaps should be followed accordingly, while emphasizing the importance of considering the projections developed worldwide.

In the CENGAVER and CENKER presentations, it was emphasized that priority was given to technologies that combine effective and efficient communication, continuous communication with the team and headquarters, compatibility with situational awareness-enhancing cameras and unmanned equipment, mobility with movement force and capability, and technologies that enhance operational

SIXTH SESSION SUMMARY

capability. It was stated that in all these technologies, priority was given to designing systems that appeal to three generations such as Generation X, Y, and Z, allow for the development of doctrines, and are suitable for their purposes.

Rear Admiral (Retired)
Hasan ÖZYURT
MODERATOR

I am Retired Rear Admiral Hasan Özyurt. My last position was the Head of Naval Operations. Subsequently, I began working as a management consultant at Meteksan. As someone who has operated an operations center, and having intensely used an operations center for two years, I have become very closely interested in the subject of digital headquarters.

In an operational environment, a high volume of data arrives, and we must evaluate this data. In a real operation, we are loaded with far more data than we can handle. As the operation escalates, data increases significantly after elements begin to deploy to the field. It has a logarithmic increase. We need to consume and control this data. Decision-makers also need to use this data in their decisions.

We intuitively know that computer technology and the use of artificial intelligence will be beneficial in this endeavor, but I believe our participants will make a significant contribution. One thing that is very clear from the digital headquarters concept is that there are comments suggesting that robots will control the headquarters, artificial intelligence will make decisions, and there will be no need for humans. How can we increase the information processing capacity of the headquarters? The task of a headquarters is to process information and generate decisions by processing it. Then, to follow up and analyze the execution of this decision. How can these basic functions be improved? Also, in our headquarters, information is still in PowerPoint or Word. We look back at a slide from a year ago and scan it. This is a time-consuming situation. It is also important to process information and keep it in a usable state. I think the digital headquarters should go beyond PowerPoint. Now, I give the floor to my esteemed professor.

Prof. Dr. Şeref SAĞIROĞLU
GAZİ UNIVERSITY

Thank you for the invitation. I am a faculty member in the Computer Engineering Department at Gazi University, and I have been working on artificial intelligence and robots for 30 years. I am one of the professors who have contributed to our country in this field. Today, although I may not be directly explaining artificial intelligence in headquarters to you, I believe that everything I am explaining will allow you to grasp the perspective that will form the infrastructure for many things here, digital headquarters. We discussed the digital world a moment ago. To understand this digital world, we need to understand the age of artificial intelligence. We talk about being in the age of artificial intelligence, but we are not actually in the age of artificial intelligence, we are actually in the age of big data. Artificial intelligence is a tool for us to evaluate the data we produce today. But let's state that artificial intelligence has gone far beyond this point. We need to understand this age of big data correctly. The shape we see here is actually the big picture of the internet. Different colors represent different domains, forming the big data foundation we are talking about.

We manage the world according to how we perceive it. If you truly see this as a data foundation that shapes our world, then you are trying to shape the world. This perception is very important here. Of course, there are significant opportunities, challenges, and threats. This forms our future perspective. When we relate this to battlefields, we must say that it is an important concept for managing battlefields and successfully implementing them. What does it mean to understand the big data world? We need to understand that even the definition of data has changed. We see here how the definition of data, which is the foundation of science, has evolved and changed, and how these changes in definitions are reflected in our lives and work. Looking back, with the concept of big data entering our lives after 2012, we are now in the age of smart big data and now generative big data. That is, machines are now producing data and we see these as an environment that evaluates this

data. We said we are in the age of artificial intelligence, and the definition of artificial intelligence is also changing. We have moved from the goal of thinking machines to machines that can now mimic thinking. In this age of machines, we know that all kinds of data are processed and transformed into a format that humans can understand. So what is there in this new age? When we say the age of artificial intelligence or big data, we truly have incredible opportunities presented by the vast amounts of data. And there are also threats brought by these opportunities. Now, when we look at this, of course, the developed algorithms offer us how to develop solutions closer to human perception.

Initially, we started with just natural language processing, the part we call "text to" when we type, but now we are in a structure where images, visuals, code, and sound are combined, analyzed, and transformed into various mediums like text, sound, visuals, and code. Of course, this structure offers us such diverse environments that structures capable of solving anything we want in every field are on the agenda. Naturally, we are also faced with great success stories. When we look at this, we see that it involves many disciplines, that the process starting with natural language processing has actually gone far beyond natural language processing, and that many aspects such as sound technology, visual technologies, and computer programming techniques have entered our lives and are reflected in our lives through large models. We know that when these developments reached 1 million users in November 2022, we actually saw the beginning of a major change in the world. I am a professor who has been waiting for this for 30 years, we are working on this, but this change and transformation, the growth of data, the processing of big data, the analysis or presentation of big data by transforming them into a vectorial form on a common platform, that is, it has entered our lives with a simple structure based on the principle of predicting the next word.

Even such a simple approach causes huge changes in human life, and today I will try to explain that to you. Now, when we look at it, the basic principle here was big data, the process started by training two large databases, which started with 410 billion tokens.

We are talking about serious data. When we say billions of tokens, if we consider that each word or phrase is expressed as a token, we will better interpret how the data sizes in the world are transferred to models. When we talk about digital headquarters a moment ago, we will better understand the importance of having the data that forms its foundation. Now, when we look at it, 410 billion tokens started in the 2022s, but we need to know that it has gone to very different dimensions today. Especially with chat gpt 5.0 becoming a product of the American Department of defence, 5.0 emerges as a strategic product and becomes a subject that cannot be sold without permission.

I will try to quickly convey to you that it is a strategic product far beyond a digital headquarters. So, what is the current state? We mentioned 500 billion tokens. Earlier, we talked about 400 billion, then 10 billion tokens, but when we look, large language models have now evolved. The process that started with 410 billion has transformed into models like Nano, XS, Small, Medium, Large, XLarge, just as we categorize clothing sizes. These sizes or this ranking or this categorization have come to a point where they are proportional to how many tokens your model possesses. Now, we said 410 billion, and we see trillion tokens have emerged. The process that started with Cloud 3 has now released 3.5. Look at the size of the model in October, now 3.5 has been released and it has 20 trillion tokens. By the end of the year, it will be 40 trillion tokens. This means Cloud 3.5 speaks all languages. We are talking about an infrastructure that speaks all the languages in the world and provides you with support. We are faced with an environment, a structure, a library, whatever you call it, that can answer all your questions in every language. Behind it, there are also large products like GPT, GPT 4.0. You follow these, their rankings may change, but the fundamental principle here is how much data you train them with. After the end of 2024, the beginning of 2025 will be the start of a new era in artificial intelligence worldwide.

Therefore, let's state that this new era, new structure, new perspective will bring us to think very differently, that they are structures that can answer very different questions. Their sizes and rankings can change because they are constantly being trained. Look, training with 40 billion tokens takes 6 months. This 6-month period means that the machines and processors you

train on are really high-energy consuming and high-speed working environments, structures working in data centers, trained models. Their sizes and locations can change, but there is one unchanging issue here. These are developments where we can see that they are growing, will grow, and that we can see many structures here if you provide data.

Chip-implanted monkeys are playing computer games, Tesla has a system that can control 40,000 vehicles, and a demonstration was made that can enter all flasher and light systems from a single point and synchronize them simultaneously. Huge demonstrations were made. It became perhaps a different demo of how the reality in the movie 'Leave the World Behind' could be made real. Neural data is now considered personal data in America, I won't interpret the details and believe you will think and evaluate it. A person's political inclination can be found from expressionless expressions, meaning if you provide your own photo, your inclination towards which party has been implemented as a project at MIT. There is an era of mind cloning, a person's digital twins are immediately created, you can go and do it on websites.

Now, there's the Da Vinci robot, a robotic surgery system. We have it at Gazi University as well, and we have a valuable professor there. I always tease him, all the data from 7,000 Da Vinci robots worldwide is combined and taught, and it can mimic our doctor. Meaning, it's now qualified to perform operations. We need to know that these are large systems that can be trained when you collect data from 7,000 Da Vinci robots. These are the basic issues behind why we say the age of big data. You can now find mines from 20 meters away, systems that increase image quality 8 times, artificial intelligences are being made. Behind this is big data analytics, and of course, we need to mention large language models. It is said that energy is not enough, the need for energy will increase 100 times to provide this data. To provide this, nuclear power plants are needed, and orders are being placed. Supercomputers are now at the disposal of ministries, the world's fastest-growing supercomputers. 'El Capitan', announced last week, can simulate nuclear attacks or nuclear developments worldwide in the areas where it is used. Technologies are being worked on that will speed up internet

speeds 3.3 million times faster than they are now. We see that steps are being taken and projects are being made to understand the universe, not just to understand the world, by taking the internet to Mars and transferring information from Mars. We need to know that projects have been started for energy transfer, let alone data transfer from space, and targets have been set. Projects are being made for an energy transfer of 30 MW, topics such as energy transfer from an altitude of 35,000 kilometers.

No one is unmoved by watching the light show of 10,000 drones, but when you transfer this to defence, you really need to think about it. You can use 10,000 drones for a purpose, it's called swarm technology. 1 Let's state that new names and concepts like drone ontology are now being given. Therefore, when you consider using this for land, sea, air, intelligence, operations, or logistics purposes, you can see many steps that will tell you how large a headquarters you have to manage this in, and what technologies the assisting tools are. There is a show side of the business, but there is also a real side. On that real side, there is the possibility to see many things here. Some of them can be mentioned here, such as hybrid warfare tactics, what asymmetric threats can do, that there may be gaps in information sharing, and that misunderstandings can lead to fatal consequences. Of course, everyone here thinks that you can create threats with advanced technologies, but I think it would not be wrong to state here that the biggest threat is autonomous attacks and weapon systems.

Looking at the developments, we are now in the era of digital twins. You are creating a digital clone of a person. Those who follow Reid Hoffman will definitely know him, if not, they should. He is the boss of LinkedIn and a member of Microsoft's board of directors. Watch him, he is chatting with his digital twin, and his digital twin is giving him advice.

This is truly a different process, but now many things are getting digital twins. People have achieved immortality in the digital age. You create your twin, and what do these twins do? They can provide your infrastructure.

This was actually first presented in a strategy report in England in 2022, which was then referred to as General AI, now

we call it Generative AI, and we can see how the foundations for the transition to super artificial intelligence, the transition to general artificial intelligence, are being laid. We are now in an era where, from any environment where you can get data, you can collect data with artificial intelligence agents and quickly make all the decisions you want in these environments. By collecting data from any environment with artificial intelligence agents, of course, let's state that you can create environments here that can also do these things from the headquarters that will assist the commander. I think you have understood from the small examples here that generative artificial intelligence can be used in all strategic and operational decisions when we think on a headquarters basis.

You will be able to transform from risk analysis to resource management, from long-term planning to systems that will make instant real-time decisions. Operationally, of course, we can bring up many issues here, such as target tracking, reviewing operational planning, or making decisions in the field. Intelligence is the most important part, you can fuse all the data you get from the field, people, environment, devices, weapons, equipment, or platforms and obtain intelligence from many different environments. Let's also add that there are environments where you can automatically receive data from all languages of the world and translate it into your own language.

Of course, if these pose a threat, you can also solve them by automating them as a precaution in terms of cybersecurity. You can also perform cyber-attack and cyber-defence in terms of cybersecurity. To understand attacks, we can convert them into a different image format and observe whether there have been attacks or changes from the image. Automation and autonomy are of course the most important parts. We also see this in drone shows with a large number of devices in swarms. Elon Musk says that making F-35s, that is, making manned systems, at this time is a waste of time.

Therefore, we need to update everything we do in terms of strategy and policy. We need to improve our technological infrastructures, change our perspectives. We need to increase our qualified human resources. In this era, we need to properly understand data, the data society, data structures, data

management in military terms, data science, the big data perspective, and the value that can be obtained from data. We need to create structures accordingly, that is, we need to understand that data is a strategic foundation.

Look, even the definition of data is changing in big data; data is defined by "V"s. Initially, it was defined as 3V, now it is expressed as 32V, even our way of defining data is changing. We separate, we understand, we try to understand, there is even smart data now. Therefore, we need to bring up the issue of using these in this era to create new capabilities and capacity enhancements. Of course, while doing this, we need to implement these by acting ethically, complying with rules, ensuring security, respecting privacy, and complying with personal, corporate, national, and international regulations and rules in everything we do.

I think that if you reconsider how we perceive things, what we need to do, and the risks, difficulties, or opportunities that may arise in the future, you will be able to evaluate them better.

Thank You.

QUESTION 1: Elon Musk, who has tremendous resources and power like SpaceX and Tesla, said something along the lines of 'it's foolish to do this in this era.' Does he say what should be done instead, or do you have any predictions?

ANSWER: Of course, there are predictions; we need to give more importance to drone technology and the concept of drone ontology. The numbers of how thousands of tanks, 5 million dollar tanks, were destroyed in Ukraine are evident. The story of how thousands of tanks were destroyed by small, 3,000 dollar drones is also being told behind the scenes. I evaluate that he is not talking nonsense, we are talking about the future in this change and transformation, we are evaluating the current findings. You are evaluating the present better. The matter is not just about drones, but it gives us different ideas about what needs to be done strategically, tactically, and operationally.

The digital environment is not limited to drones or fighter jets. But the reality is, you can use fighter jets up to certain

limits, but if you build an aircraft that can fly at 20 times more G-force, you can gain a different advantage, that's how I understand what he's trying to say. Behind it, when he speaks, we are talking about a person who provides internet to the world with Starlink, collects data from all sources and sensors, and not finding this sufficient, even works on structures that will collect data by establishing a link to Mars, understanding that universe. We are talking about a person with an IQ of 154, the highest IQ being Einstein at 160. Let me state that we are talking about someone with a high IQ, and the IQ level of Generative AI is also being calculated and is around 120. There are some debates, but there are also sources that express it as 12,000. Look, its success in code is 92 percent.

You say let's develop a successful game, you want a game, you say you want it, you type it, GPT's new product brings up the game screen, you play the game, you don't have to do anything anymore, you don't have to write code. We need to understand that we are transitioning to an era where we reach results by simply expressing prompts (short pieces of text used to guide a model or make it produce a specific response) better. The better you express it, the more clearly you define what you want, the more information and data will be behind it. The more tokens you have related to that field, the greater support a system will provide you with, whether it's by your side or behind you.

Whatever you say, therefore, such an environment also lays the groundwork for us to look at the future differently. I am sure that these kinds of events will contribute to this.

QUESTION 2: In Turkey, we are testing manned and unmanned systems. We have our esteemed Professor Feride Bahar, who says 'the future has arrived,' 'where are we within the future?

ANSWER: The future has indeed arrived, I have told you about the capabilities of 3.5. We are transitioning to the artificial intelligence era after 2025. Now, there are stages of artificial intelligence; we know that if you give consciousness to a machine, it can do many things on its own. We have entered that consciousness-giving period, and in 2025, the machine will gain consciousness. That is, let's say it can automatically do many things on its own. Therefore, this is not in the distant

future, but in the upcoming period. But of course, trillions of dollars are being spent on the development of artificial intelligence so far, and even more is being spent. Because this is not just a glimmer or a light. We have seen the sun, we know this is a major change. Everyone will be affected by this, more or less, positively or negatively. Here, we can be positively affected and benefit from it. Of course, we also need to protect ourselves from its harms, and we can express this as the biggest threat we see. In what way? Now, if you use this for different purposes, it imitates the voice and image very successfully. Look, we did a test over the weekend, I say, 'My son, how are we going to do this?' in the Black Sea dialect. It explains it again in the Black Sea dialect, it turns into a system that does this. Therefore, fraud will increase, other things will happen, which we call threats, and we need to prepare ourselves for these. The risk is not only in the military field, there is a big risk in every field, we need to prepare for these as well. That is, this is not the future, it has already arrived. There is no person I know who speaks all the languages of the world, tell me if there is. But look, artificial intelligence now speaks all languages, why? Because it is currently trained with 20 trillion tokens, and by the end of this year, it will be in the 40 trillion tokens range. That is, it knows 40 trillion words, it knows idioms, it is a system that knows many things. Its IQ is very high, it is said to be around 120, but it can answer all the questions you ask and its accuracy rate is also high. They taught it to lie, it tells super lies, there is no one it cannot convince. It has been academically tested. Therefore, we can say that everything is possible.

QUESTION 3: Professor, from a private sector perspective, in terms of technologies, in which area should we focus on artificial intelligence development in the defence sector? We are talking about areas such as air, land, space, and cyber.

ANSWER: It is necessary not to take sides here, in every field, but essentially to be on the developing side. If you can train and develop those models, the power is already in your hands. In our time, there was the He-Man cartoon, it was very popular, creating He-Man is creating the model. So, if we want to be at the forefront, we must develop the main cores of these large language models ourselves, so that we can see for ourselves what the threat will be or what will happen there. So, at least we must develop our own model.

QUESTION 4: How should we address the data dimension and the National data dimension of the work in artificial intelligence?

ANSWER: I think we understand that we need to take more ownership of our data. That is, once you lose your data, there is nothing to be done. They know everything, look, minds are being read. You enter your password into the computer, they know your password. We are talking about a system that can take the data of the general behavior of the community coming here and figure out what the general common mind here is. The system can work like a commander, it can work like a soldier. Just give the correct prompts. Therefore, it can also figure out what a country's common mind is. It also knows what a person's thought system is. Look, it can write an article in my style, defending my ideas and thoughts on my behalf. There were subjects that were said to be impossible, it was said that it could not write poetry, artificial intelligence systems that write the most emotional poems have been tested, they write incredibly emotionally. Let's be aware that our castles are being taken one by one, that our castles are gone. Artificial intelligence is such an era, such a change, such a transformation.

QUESTION 5: Ultimately, decisions will be made at the operative and strategic levels for us. However, our National interests, our cultural needs, the environment we live in, our National goals are very prioritized. At this point, is there a study on the artificial intelligence model created knowing our reality, being specific to and dominant to us, there is an international law but everyone interprets it according to themselves, it needs to be interpreted according to us?

ANSWER: Actually, just like my answer to the question of what the sector should do a little while ago, we should create our own National algorithms and large language model. Because you are feeding it with correct data, if you enter wrong data, it gives wrong answers. We call this hallucination, you know. Therefore, it is necessary to feed it with correct data, because it learns what you give it in the learning environment. If you express National moral values, national interests, other issues, it arrives at results accordingly. Look, even if there is international, wrong data given, you cannot explain the issue if you do not do

the Armenian problem with your own data, because the system answers that way. The new generation will learn this way, either your national interest or libraries, data on truths, those environments need to be created immediately. There is no 'I don't know' in its algorithm, it gives the closest answer. I have never come across it saying 'I don't know'.

QUESTION 6: How will we trust artificial intelligence outputs in military operations, despite the risk of making mistakes? Do artificial intelligence languages communicate with each other, do they talk?

ANSWER: Can a commander use it? The answer is yes. Because the commander makes decisions with the data in front of him. The healthier the data the commander receives, the more accurate decisions he makes. Now, if there is a system that instantly processes all the data coming from your network and presents you with information, we call this big data, analytics, that is, artificial intelligence systems are also integrated into this. Therefore, the commander can make more accurate decisions at a higher level than the other decisions he makes. A second issue, agents talk to each other, that is, a single system does not work, it also communicates with other artificial intelligence systems. It also receives data from there.

QUESTION 7: Sir, you mentioned 7,000 Da Vinci robots. It is not possible for us to escape from technology, we experience technology in almost every field, from banking, in military forces or internal security, border security, almost everywhere. The watch on our wrist, the laptop. I see the following as a problem and frankly I am afraid. We are talking about 7,000 physical robots, we think that these robots are under our control under normal conditions, we control them. But isn't there a danger, what will happen when they talk to each other and produce their own languages in the future, can we foresee this?

ANSWER: What we foresaw has already been done. They can think among themselves, such a thing happened and the subject was closed. We can think, of course, that it can be a threat. That's why we are here. To talk about them. We think that we need to focus on where there is a weakness behind these destructive threats, where there may be a problem.

Major Emre AYVAZ
Ministry of National Defence

Major Emre Ayvaz, with your permission, sir, I am the intermediate section supervisor of the Air and Space Power Development Command. Our presentation is on the content of the War Game Planning Tool (SOPA). As the Air and Space Power Development Command (HUGEM), we are working on developing the transformations needed by the Air Force Command to maintain being a respected, effective and deterrent power in the region, following the unprecedentedly rapidly developing technology, and researching the effects of the paradigm shift experienced in every field with the effect of artificial intelligence on military aviation in this context.

When we look at what a war game planning tool does in this context, it is a living system where all the variables, all the tokenized variables we mentioned earlier, are included and dynamically transferred to the system in real time to defend Turkish airspace. SOPA will actually be the first step of this. We will share our views on what can happen next. Of course, this structure will be an application where we can use systems such as exercises, operation plans, war games. It is actually a structure that forms the basis of cloud systems, which we call micro agent-based. We are talking about a structure that can support general artificial intelligence by producing more cost-effective and more realistic results every day. Of course, there is actually a dimension of this that goes to the virtual universe dimension. These, which we call the first step, are simple simulation applications. But a step beyond this is the virtual universe, that is, the system where trillions of dollars are currently spent, Meta and similar ones, where Mark Zuckerberg has invested more than 40 billion dollars in 3 years and continues to increase. The virtual universe offers us dual-use. We have always talked about the military dimension, but in civilian events, fires, earthquakes, disasters, humanitarian aid, from the initial shock phase to the planning phase, to decision support, meteorology, finance, internal security and even politics, it gives an incredible vision to decision makers, we are

talking about a structure that processes the huge data called ZettaByte, where huge cloud systems work in the background.

Of course, there is a need to establish data farms, data center farms. NVidia company has sold all of its products that can be produced until 2026, that is, they are all reserved now before they come out of mass production. Because these are no longer biological intelligence, they are digital intelligence purified from biological intelligence. It is really close to impossible to prevent these systems. So, when we prevent this, it is foreseen that we will unfortunately suffer from its problems in the future. I will also talk about a process where the air force foresaw this 25 years ago and our valuable commanders who are in a decision-making position about this are here now.

So, what are the technological developments in military aviation? As far as we follow, as far as we see, we know that even 5th Generation aircraft, which have been in the field for a long time, process terabytes of data in the air in a single sortie. So, in fact, it is not just aircraft in the air. We are also talking about machines that perform data fusion, evaluate it, and present the pilot with as much data as he needs, without harming his awareness. Quantum communication is now theoretically implemented, and we even know that it is practically implemented. We know that we can do it with small applications in Turkey as well. What is quantum communication? It provides 100 percent security, the most important thing in the military is security. In civilian life, the opposite is true, functionality first, then security. But in the military, if there is no security, there can be no functionality, if it is not secure, everything is trash for us.

We are looking at other developments, incredible developments in UAVs, micro and nano sizes, laser systems or hypersonic missiles, which we call directed energy weapons, space, satellite systems, cognitive electronic invisibility technologies, surveillance, radar systems, incredibly rapidly developing systems in many areas. We are talking about a structure that is developing so rapidly that even experts in their own field cannot keep up. The basic catalyst of this is artificial intelligence. Even the latest version of our current ChatGPT writes code at an incredible quality and speed, which is a much more primitive version than the software used for defence purposes. I have been writing code for 20 years, I think it is impossible.

We express chip technologies by saying 2 nanometers. It is easy as a term, it is easy to say the terms, when we look at the details, it is an incredible technology. What we call 2 nanometers is actually the size of a DNA molecule, a strand of hair is 20 thousand times and 30 thousand times this. That is, they produce chips at this size. A chip is 20-30 thousand times the size of a DNA molecule. There are studies to reduce this to 1 nanometer.

When we look at the satellite change in the sky between 2017-2018-2019-2020, we see a rapid increase every year. Nearly 40 thousand of these are in near orbit, nearly 10 thousand are in the middle region, and the least are in the outermost layer. There are so many satellites, like an ant swarm, that if you throw something from above, it will not fall down. None of these touch each other, they work continuously simultaneously. We can see the development of the dimensions of technology since 2017 with these figures. We can actually say that it is one of the capabilities that artificial intelligence has added to this area, and this number is expected to be 57 thousand by 2029.

Let's look at the importance of numerical data and the interpretation of data. Petabyte, Exabyte above it, Zettabyte above that. In short, data is growing so fast and is so valuable. We have machines that will process these 24/7 without getting tired day and night. We have algorithms that can bring awareness to these, establish context like us, establish context better than us. Therefore, this is truly a very important area for the Air Force that stands before us.

When we look at the technological requirements of the near future as the Air Force, we assess that the definition of the need will generally be small, fast, effective, online, that is, continuously communicating structures that communicate within their own network. What will our needs be in operations centers? We will need systems that can make predictions and provide decision support at the microsecond level. Again, quantum encryption will be very important. If the encryptions we currently use will be trash, which quantum computing provides a mechanism for, we can say that it is not our current communication tool. Because we have asymmetric encryption methods and quantum can solve this very quickly. Therefore, we will need quantum key distribution and encryption. As I mentioned before, we need nested developed networks and the ability to configure their different permeability security levels.

These work well in two dimensions, but there is serious confusion in the air and space dimensions. We must calculate many parameters such as magnetic fields and solar flares, and these are critical sensitive issues in communication.

And again, terabytes of data flow per second, that is, below 10 milliseconds, 10 milliseconds is a perception level that humans cannot understand, we humans can react up to 200 milliseconds. That is, predicting the future with a structure that will create a virtual universe step by step as a result of designing simulation systems in a real-time interoperability environment with training exercises and strategy development. We are enjoying the blessings of the Air Force Information System, a very valuable decision given 20 years ago, as I mentioned earlier. Many management tools of the Air Force operate on the air force information system and all corporate data is exactly where it should be. It provides very good functionality with a method we call business intelligence and perfectly fulfills our corporate memory. That is, systems that do not have an infrastructure to describe a world as chaotic as the deterministic and how accurate the information it gives is for the war game planning tool.

As I mentioned earlier, we are talking about improvements that will become more realistic every day. We think that if ASELSAN, which will develop a system, does not create a digital twin of that system according to this interface today, the chaos we return to 15 years later saying 'I wish we had done it all' will increase incredibly. Therefore, a project started today will ensure that everything is done according to this project and we evaluate that it will bring us great advantages 10-15 years later. We think that the system will be a living system with improvements that will become more realistic every day, and that it will provide an infrastructure that can integrate developments in virtual reality, augmented reality and mixed reality technologies within the scope of human and machine interface between the real world and the virtual universe. We said that this system will offer both cost-effective and much more realistic solutions in training exercises and intelligence. It will be a study that will provide great benefits not only in the tactical field, but also in the strategic and operational fields, land, sea, air, space, cyber, social operations and electronic warfare fields. In addition to conventional operations; It will contribute to the configuration of hybrid environments

(physical and virtual environments), gray zone conflicts (indefinite and irregular wars instead of official wars), information manipulation, cyber attacks, economic pressure, social engineering, etc.), non-kinetic effects, CBRN scenarios and various natural disaster scenarios.

We will have a structure where we can even implement non-kinetic effects, that is, Chemical, Biological, Radiological and Nuclear (CBRN) scenarios. So, what will we need? It will be produced with things that have a virtual sphere and physics engine, can expand horizontally and vertically, are microservice-based, can pull information from big data and combine the validity of the pulled information in a blockchain-based database after it is completed, and can actually be accessed as 3rd party applications. But when these are used for military purposes, they will need to be Nationalized. If we plan a perspective and regulation from today, guide our defence industry accordingly, we say that the virtual sphere and physics engine of a structure whose infrastructure is gradually being established from today can be Nationalized over time. It is not easy, these are time-consuming processes like integration, but we evaluate that it will accelerate with artificial intelligence. It must be able to process data from open source and have such a module. It also needs to respond to real-time intelligence, simulation of multi-layered networks and cyber security needs. In the development schedule heading, we are talking about a structure that will be living, developing like us and continuously learning, learning chaotic processes and supporting decision-making, which is what the Metaverse is today, what we will do as a country or company. But we evaluate that there can be a virtual environment where complex military and civilian scenarios can run within 5 years.

As a result, it is important to transform technological developments into the most effective forms for national security. When we look at industrial revolutions, we are talking about industrial revolutions that happened in 100 years, started in the 1800s and are now happening every 5 years. We see that quantum technologies, which will come in 2030, have started to enter the field today. This is a structure that humanity is not very used to, there has never been such a rapid development and we evaluate that this structure will continue to accelerate due to tireless machines.

In this context, we think that there is a very fundamental need for a Turkish large language model, especially in the field of artificial intelligence on a global scale, that we will go somewhere by using ready-made models today, but we foresee that similar problems will be experienced if there is no Turkish language model, just like we would not know what to do in a difficult situation with the F-16s we used in the past.

We also evaluate that being part of the investment race in the virtual universe and quantum technologies is valuable. Indeed, we can actually get some clues from the fact that all of the large companies that direct technology, the so-called Magnificent Seven of America (Apple, Microsoft, Alphabet, Amazon, Nvidia, Meta and Tesla), with a valuation of more than 10 trillion, have completely turned their direction to this.

In air forces, which closely follow technology and mandate the use of the highest technologies, the adaptation and effective use of the technologies in question are vital. It is evaluated that the effective use of such capabilities will provide information superiority to the commander on the road to certain victory in an operational environment where the developments in artificial intelligence and virtual universe technologies, in particular, are indispensable for supporting decision support functions. We are talking about the capabilities of Boston Dynamics' Atlas robot, which can make autonomous, Cyborg-like, superior movements than humans, and can turn its head 360 degrees or 180 degrees. I think this is also one of the indicators of where technology can go.

Thank You.

QUESTION 1: We are very security-conscious in the management of large databases. You have also started a study on artificial intelligence. What is your current prediction, will we feed our databases only with our own data or will we get support from large databases? If we continue to feed with our own databases, will this be enough for us, what is your current position and thought in the setup?

ANSWER: Data base is a subject I am knowledgeable about. We take the data, and just like a human, extract and put summary data as a human processes it. That is, the ready-made models we use are actually fed with summary images from these huge data sets as a result of the processors' work. The reason why we get a response in milliseconds when we write is that those questions have actually been asked before and their vector has been extracted.

Therefore, the more data you process, the more advantageous it is. Therefore, the more data you process, the more advantageous it is. All our data is currently going, from the cell phone to the wristwatch you wear. They take all the data and we cannot stop it. That is, stopping it is an unavoidable situation due to democracy and similar methods. They follow all your routines, what time you will get up in the morning. If there is a need, that data is there. We are talking about systems that will know you better than you know yourself. We should not open our databases. The greatest strength of the army is working on a closed network, a closed network is really very difficult to do something. But everything can be done through those cables, but the closed network is one of the things that best protects the army. This should always continue until when, maybe until we switch to quantum, because quantum provides undeniable security physically one-to-one. That is, just as we are sure that an apple will fall to the ground when we drop it, we can provide the same security to communication with quantum key exchange.

QUESTION 2: Should humans remain inside or outside of critical decisions with artificial intelligence?

ANSWER: Artificial intelligence is taking baby steps. What the internet or Google was in the 1990s, when it first came out in the 2000s, these are the first steps of artificial intelligence today. Therefore, it is being talked about reaching artificial intelligence at the maturity level. A situation like 'I saw a new light, my ignorance was enlightened', actually means that we have established a better structure than all the experts in every subject in the world. A system that can give information and do it very quickly. It can also be thought of as a genie of Aladdin, that is, a genie coming out of a magic lamp. We are really talking about a group of machines that can do many of the

things we say. So, humans will of course be involved in making decisions. Because at one point we will use it for our own interests. But the less it is, after a point, it can choose the most correct probability out of billions of unseen probabilities over time. Therefore, we may want to leave the decision to it over time.

Fatih Bilge İZGİ
HAVELSAN

Welcome everyone, I am Fatih Bilge İzgi. Before explaining the Harbiye product family, I would like to emphasize that I am also a graduate of the Military Academy. I graduated from the Military Academy in 1991, retired from the Turkish Armed Forces in 2015, and started working in the HAVELSAN Command Control Information Systems field in 2016. We act as a bridge between the engineering side, which is the kitchen of the work, and the authority that is the needs authority and the supplier authority.

On this occasion, I would like to thank the SASAD organization for giving us the opportunity to provide information about our Command and Control system, where we have tried to reflect our gains from the Turkish Armed Forces, which enabled us to grow in this field.When we talk about digital headquarters, of course, everything is digital, zeros and ones are flying in the air, there will definitely be forward-looking approaches. As our EDOK commander, Lieutenant General Zorlu Topaloğlu, said yesterday, we have to act proactively. While acting proactively, I will introduce our Operations Information Management and Integration product family developed by HAVELSAN in terms of what we have done in today's solutions. Meanwhile, within all these narratives, another important issue that we are trying to realize from our point of view is the interoperability solution. Also, at the point of providing contact with other standards developed or models, systems, capabilities produced in different parts of the world. I will also try to convey the approaches developed by HAVELSAN in data analysis. Our product family actually consists of Harbiye at the strategic level, Headquarters, Harbiye Tactical at the tactical level, and our Harbiye TEK-ER application at the TEK-ER mobile level. Integration between these is also a part of this solution. We are focused on solutions for tracking current operations in the Operations Center. Therefore, we are focused on tracking and managing current operations through classical situation maps, from where we also provide our command and

Control capability. We track both friendly and enemy situations in this way. Of course, one of the most important tasks of the headquarters is actually to make decisions. The product that results from this decision is actually either a plan or an order. It may be a plan that turns into an order or it may be a direct order. But here, the ability of the entire headquarters to make decisions on the annexes, drafts, and tables of the same plan or order in a common, that is, parallel way is also an important capability. Not only plans and orders, but also headquarters situation assessments and directives are part of our capability. We also need to focus on organizing for combat here, because while executing a combat or a long-term combat, there must be a normal flow of information. We also need to create and publish the organization for combat in the system, which we can define as the organization we have temporarily switched to for a special situation, within the system and publish it to the lower and upper units, so that we know what kind of formation we will be in in the middle or at the end of the operation, at every stage.

Of course, military symbology is very important while all of these are being done, and military symbology here requires a standard. Especially when you look at situation maps, like a note, just as it is universal all over the world, operators in all different fields of interest should understand the same thing. Our collaboration tools, briefing preparation tools, applications where elements in very different headquarters, which are temporally and spatially in different environments, can work on a whiteboard as if they were in the same room on a whiteboard, also enable us to collaborate. The transition phase from struggling with PowerPoints to command control information systems. At least it started in the Land Forces Command in 1999, after the first and second management phases, the 3rd phase continues. There are also very good developments in the field of Command and Control on a Land Forces basis.

Of course, artificial intelligence is very important and progressing in the prevention of conflicts, but we also need to have a conflict prevention capability where humans are still at the center. That is, when you look at a region, we also need to support and work with information coming from different verification channels, which makes it easier for the commander when he looks at it, at the point of whether this is it or this is it.

Separate working modes are also required in these headquarters environments, in such headquarters-oriented command control systems. Because you are managing an operation on one hand, exercises continue on the other, you are providing training on the other, and you are developing highly classified plans, general defence or attack plans completely independently of the outside world in cosmic rooms. The application should have modes that respond to all of these. We can also provide multi-language support.

In the process of preventing conflicts, it is also very important to be able to identify whether a piece of enemy unit information that has come from multiple verification channels and multiple news channels in a region is really the mentioned enemy unit or a different enemy unit. That is, we also have the capability to enable us to move from unconfirmed data to confirmed data and a confirmed situation map in military jargon. Replaying the mission is a very important capability. Because especially in post-activity reviews, shift briefings, it is necessary to master the retrospective data. Mastering technologically is the field of engineering, but mastering operationally is also an important input in shift briefings and post-activity reviews, and in evaluating the process of what we did and what we could not do after a major operation, through these features. You give tasks to the units, these are all done with tasks, you know we say command, command, command. But underneath, you actually start throwing tests down with engineering, and you start throwing tasks in the operational world. And it is very important to visually track these tasks well, which task has how many tasks in each other. It is also very important to have the feature that can say which tasks can conflict, be aware.

In addition to standard reports, such as shift reports, reports required, and daily reports, reports specific to the person's own working style, needed, or developed specifically for themselves can also be provided by the system.

We also use NATO's standard messages as a capability. Our GIS (Geographic Information Systems) capabilities, that is, map analysis capabilities, are also delivered not only to the wheel or tactical field, but also to operational and strategic, that is, brigade and above centers. This also provides us with

great convenience. In addition to field situation and visibility analysis, we also have solutions that offer selection alternatives such as which way to proceed and how much force. When integrated with HAVELSAN's CBRN capability, we can also provide predictions about these situations.

One of the things we need to do to act proactively is to actually join the community. That is, everything has a community. I went to a darbuka course, though they call it percussion. For example, it has a different community, the man told us. For example, a darbuka starts from 22 cm and goes up to 26 cm. In fact, he said that you were ripped off for the darbuka I bought. Because I couldn't fully join that community, because it also has its own standard, the darbuka community. Advanced Command and Control systems also have a community to follow. A very good question was asked in the previous session and my teacher gave a good answer to it, 'There are developments in many areas, in which area should we, as the private sector, develop, which way should we turn?' To the question, our teacher said, 'We should be on the developing side.' The condition for us to be on that 'developing side' is first of all to join a community. What is the second condition, you will go there to do something. You also need to master the subject to do something. In the first meetings, you go and sit in the back, you wonder if you should raise your hand, will it cause trouble for me. But after a while, when you gain experience, you start to be active, not passive there.

You start giving change proposals and they start saying, yes, we didn't think of this. What do we think when we give this? What we need on the National side. Because there is a model, there are models we follow. There is also a model we follow in the land domain.

MIP products (Mutual Interoperability Program). What there is, there are models, data model and data exchange model. As a result of our inclusion and effectiveness in this, we also have the necessary changes made in these models. What do we follow, NATO standards. NATO has many standards, but we especially follow the standards that it has packaged all these standards in the Federated Mission Networking (FM) side. We are currently working on the standards that will be put into operation in 2030 and we are contributing to them. Sometimes

we exaggerate the issues as to whether we can be a part of this, but you can be one of the 3-4 partners who act bravely at the solution point, like Havelsan. What are we doing in that position right now in terms of acting proactively in an upcoming standard? We offer solutions to that standard with our own applications, and we also offer our change proposals at the point of the maturation of the standards. Where are we going? We are going to international NATO exercises, we are going to CWIX exercises.

At the end of each year, you see the focal points where NATO's actual output is taken, and here you see the focal points. Here, air, land, sea, cyber, and this year, topics such as modeling and simulation were also included. We are talking about multi-domain operations, beautiful projections, projections that will see the future. What will NATO do in 2030? When you are on the development side or the labor side of the work, you see that the focused area in this year's CWIX exercise is Multi Domain Command Control. That is, these issues start there, some projections are made, designed, it is said that it should be like this, like that. If you are there, you are involved in these processes. We have always been involved in these, we have passed all the tests successfully by being involved in various versions in the 2018, 2019, 2021, 2022, 2023 periods. Why do you pass, they are also looking for this from you and not only NATO countries are looking for it. They want a capability that meets the standard.

What we call Harbiye Tactical is a solution at the battalion and lower levels, mostly in narrow bandwidths, at points where communication capabilities are more limited and where you are more mobile, that is, at the tactical level.

A solution where the capabilities of the headquarters solution are reduced, but some capabilities, that is, tactical capabilities, are further enhanced. Because especially in situations where we need to be more sensitive, such as unit tracking, target tracking, close tracking, the capabilities are included and again a system that provides you with communication capabilities in a narrow area. We again define messages, manage current movements. For example, there are navigation and assignments. That is, a capability that we do not need at the strategic level is included in the tactica l as an

additional capability here. Because there may be a need for navigation analysis in the field. Again, you need to have a moving map so that you do not constantly update the map.

Here, friendly and enemy situation information comes to the fore much more. Because here, the entire system is fed with the inputs and data you give. The data for most of the steps taken by that headquarters we call the headquarters to make its decision is provided from here. Since we are mobile, let's integrate with the systems on the vehicle itself, integration is also provided up to the number of ammunition in the turret and the elements detected as threats in the vicinity.

When we come to mobile, it is a mobile cell phone application. It also has additional capabilities on it. The roles in the CENGAVER formation and the required capabilities are also included in the whole system. Messaging and sensor data are also available in our mobile application.

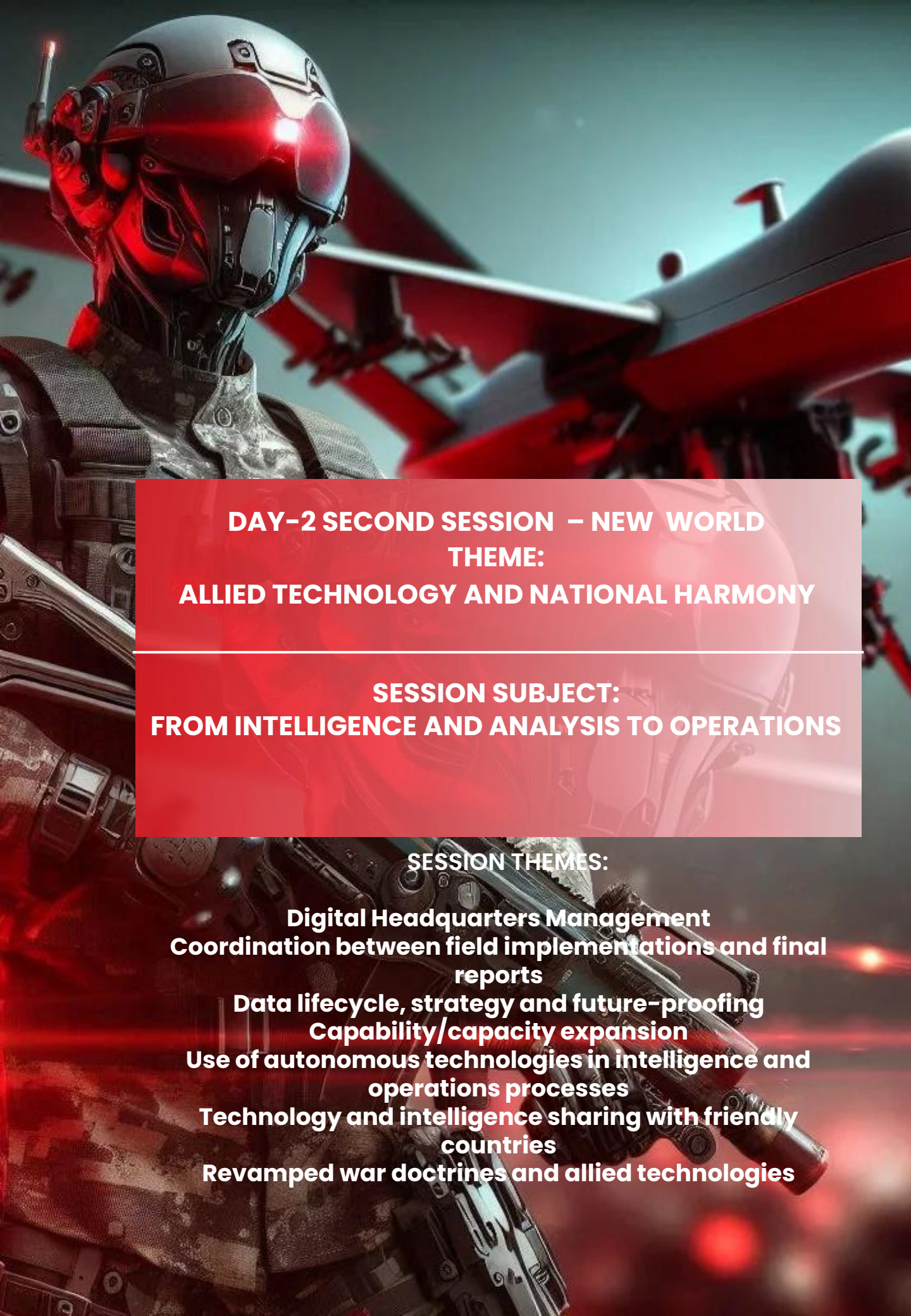
In the interoperability solution, it offers solutions for systems created with different standards, or systems created at different times, or systems using different versions of the same standard. In this way, we provide very different gains such as financial dimension, savings, joint solution and cooperation. Here we offer you a powerful integration capability with Octopus. That is, without interfering with the areas where different systems are developed differently, without affecting their freedom, you can say that I get and use different data from different systems. When you do this, the entire integration work is already handled by a separate capability. If all command and control systems also deal with integration, an extra burden is placed on them. Managing this area as a separate capability pool saves time and money. We have a similar approach in data analysis.

That is, what we actually need is balanced news and data within the information gathering plan. This is a need and how should it be provided? It should be provided correctly and on time, that is, if you provide data incorrectly, if you provide it at the wrong time, it will not work. If you provide the correct data late, it will also lose its currency. Therefore, you need to provide it on time. For this, it has been developed especially to assist the operational user in these information gathering processes.

All sources are scanned in the architectural structure. By processing text, web, social media, images and videos, both written and visual information can be extracted and presented to the end user via web, desktop application or mobile. In text information extraction, you prepare a set, when you say this region, these data are needed, it delivers the data to you at that time, in the past, in the advancing times of the operation. If needed, it also does language translation and also classifies. That is, it does not just take the image of an internet page and give it to you. It does that job much more detailed on your behalf. Visual information extraction is also the same, for example, in the Naval Forces application, it reveals and presents to you the main features of a ship without your involvement. It presents not only visual but also textual information. It can also separately present data that is in the image but not in the text. Data preparation work, you must prepare the data very well for all these systems so that they give you good results.

The focus of the data issue is to present the correct data, the necessary data and the timely data to the operator, commander or decision maker.

Thank You.



DAY-2 SECOND SESSION – NEW WORLD
THEME:
ALLIED TECHNOLOGY AND NATIONAL HARMONY

SESSION SUBJECT:
FROM INTELLIGENCE AND ANALYSIS TO OPERATIONS

SESSION THEMES:

Digital Headquarters Management
Coordination between field implementations and final reports
Data lifecycle, strategy and future-proofing
Capability/capacity expansion
Use of autonomous technologies in intelligence and operations processes
Technology and intelligence sharing with friendly countries
Revamped war doctrines and allied technologies

SEVENTH SESSION SUMMARY

Attention has been drawn to the importance of determining how to use which data for the risks that artificial intelligence can bring in the collection, storage, security, transmission and interpretation of data. While it is stated that artificial intelligence imitates the given data in its current period and has not yet reached the stage of giving an original idea, it has been recommended to focus on working on different alternatives due to the risks that the army cannot afford, especially in this period.

While it was suggested that priority could be given to different statistical methods and software, it was recommended that methods such as data filtering or sensor fusion should be preferred according to their fields. Taking the F-35, the 5th generation aircraft example, it was stated that artificial intelligence could be used for image processing, but kinematic vector, sensor fusion solutions for data such as target detection, tracking, situation vector, where it is, could be more useful in terms of both security and data load. It was emphasized that these methods, which will be integrated with human feedback, will provide more accurate decisions in artificial intelligence model training that will make decisions. In addition, in the TUSAŞ attack example, attention was drawn to the risks that the fact that the building plans are available on the internet and the lack of software or filtering to prevent this can create with military security, while concerns were expressed that environments where artificial intelligence can say 'I did not understand this' in critical situations can create risky situations for short and medium term periods. While it was requested to increase cooperation on data sharing in order to test such different solution proposals, it was stated that if this problem is eliminated in the development studies in academic studies, the processes for developing products, projects and solutions can be accelerated.

In the last section, modernization and transformations with topics such as space, satellite, network centers, and artificial intelligence were exemplified with studies worldwide.

While sharing the changes in war environments with technologies, the changes in the command-control level, and

the predictions about the use of technologies in the future war environments, it has been shared that autonomous helicopters, autonomous tanks, artificial intelligence information systems, unmanned systems and swarm technologies will renew doctrines at the strategic level, operational level, tactical level and engagement levels. It was emphasized that the one who structures information, observes, directs, decides and makes decisions the fastest will have the greatest competitive advantage. With the emphasis that the greatest unchanging reality in wars is the doctrine that 'there will be no combat without combat', attention was drawn to the importance of capturing the electromagnetic spectrum, while it was predicted that swarm intelligence would primarily target such targets. Attention was drawn to the importance of developing asymmetric response technologies by closely following rival technologies.

Lieutenant General (Retired)
Nihat KÖKMEN
MODERATOR

Hello, I served as the Head of the Air Force Staff and the Head of the Turkish Military Representative Delegation (TMR) at NATO. My articles are published in think tanks related to my field of interest. Regarding my interest in technology, in the past, when I served as the Head of Plans and Principles at the Air Force Command, we worked intensively on the projects of our Air Force and future-oriented predictions. We have accomplished many of these. Although we talk about unmanned systems, autonomous systems, drones, I am still one of those who believe that manned systems are the main striking element of our forces. On the other hand, I served as Deputy Undersecretary of the Ministry of National Defence between 2010-2012. We worked on the Göktürk-2 satellite launch system. We worked on the sounding rocket, and we contributed to many projects such as the penetrating bomb and CİRİT with our valuable colleagues.

Of course, we see that artificial intelligence has entered our lives and we know that there is no escape from it anymore. It has entered our lives with daily technologies. But of course, I would also like to emphasize that we, as soldiers, have security and survival. We are starting our conversation session. Intelligence and analysis were clearly expressed in the theme of 'Allied Technology and National Harmony'. Of course, intelligence is one of the most needed issues in the operational environment. We can all imagine how important it is to obtain, store, transmit, store and deliver this intelligence to field users and decision makers.

Doç. Dr. Ahmet GÜNEŞ
GEBZE ÜNİVERSİTESİ

Hello everyone, the first step regarding the use of data in the headquarters or anywhere else starts with looking at the data life cycle. Of course, the next step is to determine through which channels we will transmit it, data storage and data security, determining data access restrictions and finally what we will do; interpretation and analysis. After collecting the data, the first part of the data to be looked at is the quality of the data.

We need to look at what we want to do with the data, why we collected this data, and whether this data is consistent within itself. Can we work with these same data in another operational region in a different way? That is, what kind of problems can occur in the environment change, these parameters need to be evaluated.

When evaluating data quality, there also needs to be human quality there, so that when they look at the data, we can be guided. If we look at what our intelligence sources and data sources are, we can see areas such as communication-based (SIGINT), electronic warfare and intervention, image analysis, geographic intelligence (such as satellites, GPS data), cyber intelligence (online activity, social media, intrusions), acoustic intelligence (sea and underwater threats) and biometric intelligence (city security, Mobese). Electronic warfare is a very much talked about topic in Turkey. When I took a brief look, I saw that almost everything was made into intelligence by adding INT to the end. Especially in this data collection part, Turkey is not bad. It is possible to get data from different sensors from different channels. From MOBESE, Infrared, to unmanned aerial vehicles. Only acoustic intelligence may not have been heard much. There, it is mentioned about collecting the acoustic signatures of ships. After the data is collected, things get complicated in my opinion. Attention should be paid to issues such as data encryption and cyber security. However, my major said in the previous session that 'We, as soldiers, are in favor of protecting our data'. Okay , that's great, but we, as

engineers, need this data. The problem here is security or ease of work?

We are not talking about going and giving critical information for the security of a very secret country here, but a layered access can be defined, easier access to such data can be defined for researchers and companies by increasing encryption and security systems.

Because, for example, hyperspectral image processing, the subject is not very difficult, but the sensors are very expensive. Only one or two companies in Turkey can work on this. But perhaps if we could define some toy problems with the private sector and distribute data, we would be able to get more data from many more companies. There are similar problems in underwater acoustics, sensors and vehicles, devices are very expensive. I think there are similar problems in aerial images as well. There is such a dilemma. We are excessively focused on the security side.

By the way, in the analysis and interpretation part of the data life cycle, we received the data, is our data correct, is there an error? For example, you are expecting an infiltration from somewhere, you caught 10 people with the camera, but the radio communication increased 10 times on the inside of the border. It means we missed something. It is very important to look at whether the data we have is consistent and whether we are making mistakes. Pattern recognition is the name of the courses in computer and electrical engineering. Correlation or anomaly analysis within the data itself needs to be done. Unfortunately, we take the data and only use it for visualization. The title of data analysis is visualization, but we generally stay here. We are like this not only in the defence industry but also in the industry 4.0 field. We are in a situation where digital data is only used to report to managers, and that is why our ranking in digitization indexes is certain. So we got the data, did the preliminary analysis? The issue I will specifically address is this. We go to bed with artificial intelligence and wake up with artificial intelligence, I am also working on the subject.

However, now we will do anomaly detection, for example. What happened, there is a deviation in the data in a place. For example, there is an activity in a place. Something unexpected came out in the images. Instead of producing an artificial intelligence-based solution here, it is possible to solve most of

the work with solutions at the high school student mathematics level. Moreover, there is a possibility that artificial intelligence can give you things that do not exist. In what you do with statistical and mathematical methods, it says 'there is an error', I will suggest to you, it will say there is an anomaly, let the headquarters still make the decision, let the person in charge make the decision.

There is a problem with artificial intelligence, artificial intelligence imitates, its main task is to imitate the data you give. It does not bother to find something very original. I'm not saying let's not use it, does it increase efficiency, yes. But you don't know what to do when you go to the field. For example, Tesla's accidents and the people who are victims can also be included in these trainings. There is still no autonomous vehicle on the market. So we will try to readjust according to the data that comes. Now, since this is not a risk that the army can take, it is necessary to think carefully about where and how artificial intelligence will be used.

I say it once again, many of the current problems can be solved with standard, more traditional, more mathematics-based methods. For example, Boston Dynamics makes robots. I also work on reinforcement learning. These are algorithms generally used in robots and autonomous vehicles. Boston Dynamics does not use reinforcement learning in its own robots. Why, because control and optimization are enough for the guys. Now it seems like we are missing this a bit. You have the chance to filter the things you need with LLM in data filtering. You give the data, it gives the important parts. On the other hand, you can also do this with statistical methods. In alternative methods, sensor fusion is one of the critical technologies used by the F-35, the 5th generation aircraft. Why? A lot of data comes from too many sensors. Aircraft also need to communicate with each other. Artificial intelligence is not used here either. You can use it to process images, process signals, but you have to use sensor fusion algorithms for target tracking, detection, where it is, situation vector, kinematic vector.

It was said that there are deterministic tools ready for operations. Scenarios can be developed where multiple competing elements are trained and compete with each other. As far as I know, SSB also has such projects. However, I do not know where the end of those projects goes because they are

deterministic? However, we have the chance to set up scenarios in the environment and solve problems specific to Turkey. What I mean is, the main issue is, we say 6th Generation jet aircraft. While America is trying to develop this in the South China Sea with the fear that the Chinese will attack Taiwan, should we do this when we have other problems here, or should we develop our own specific technologies? Should we develop technologies for this?

Therefore, we can make analyzes with such approaches. Finally, in these LLMs, in these models, artificial intelligence learned in simulations. We bought a new tactical weapon and it suggested a tactic to us. But you see that you make the comment that it does not work like this here. It is also possible to train decision-making models by giving human feedback to this. This is what was done in the latest versions of LLM and Chat GPT. That is, we can train them with feedback.

The use of autonomous systems for intelligence is actually more of a necessity. That is, it is not possible to not mention the Ukraine War in a panel on the defence industry. At the beginning of the war, TB2 was used, but now we cannot see it. Why? There are some problems due to Electronic Warfare. Now, one of the critical points here is that if you have to control the unmanned vehicle with an operator, the other side can break that connection. The moment you switch to communication, you are already saying that I am here, and there is also a problem with detection. Therefore, using autonomous vehicles is of course more logical in terms of intelligence. In addition, autonomous vehicles can work for much longer because they do not require a personnel to wait at the beginning.

It was a news about 2 or 3 months ago, I guess, it may have been longer. It has applications in marine water vehicles, since we have communication problems underwater anyway, since we cannot use electromagnetic waves. The Americans flew a fixed-wing system powered by solar energy from Guam to Taiwan or the Philippines. That is, unmanned and autonomous systems that can go. Payload, that is, since you have started such a study in the field, the use of these in swarms and the use of autonomous vehicles in distributed systems has also become widespread. Also, I have unfortunately not seen much use of self-learning systems in software. What I mean is, we have a study in the private sector, in mobile games, when the model gives purchase advice, or as a game or software.

It learns by itself and can make decisions based on who bought it when. However, in military systems, I put the software, it scanned the internet, for example, TUSAŞ had an explosion 3-4 months ago. Then it was said that the building plans were available on the internet, the architect put it on the internet. So why didn't a software go and find this and say there is an anomaly here?

Now, shouldn't these normally be able to be done? Now, this is what I mean by self-learning systems in software like this. At least a model should say, there is something strange here.

Of course, there is a place where artificial intelligence or other technologies will be used. The internet is a sea of seas, social media is a sea of seas, of course, you need to throw bots here and do your analysis automatically from there. NLP is especially something we will need in data analysis, it has some capabilities to make inferences. But for example, is it possible to use LLM for command recognition in noisy environments, in helicopters? Is this necessary, I am skeptical. Different methods may give better results. We, as a university, are working on this, but we are working to give an answer if asked. However, putting this into something that will be productized is debatable, how reasonable is it? Because if your LLM says I didn't understand this, it is closer to this command and makes a decision, what will you do? In the preliminary analysis, by making predictions of scenarios, for example, we put sensors, multi-static radar in a certain region. Yes, it is very logical to use artificial intelligence for the analysis of where an attack can be made here. This gives the framework, but a human definitely needs to be there to check whether artificial intelligence is making a mistake somewhere, for approval.

Finally, in the sensor fusion part, sensor fusion technologies, that is, other algorithmic approaches, need to be done. For example, biometric data is taken in the Mobese system. Face and license plate are recognized. If you remember the explosion in Ankara, that is, it has been almost 10 years, in Kızılay. There, a vehicle with a Şanlıurfa license plate passed through Kızılay 7 times, we learned this from the news. At that time, I talked with a police chief about the possibility of creating an algorithm for this. Anomaly detection can be done, it is presented to you that there may be a problem with these or those license plates. The answer I got is this; 'I can already find the license plate I am looking for. I need to tell you which of the

1 million license plates to look for.' These systems are algorithms, artificial intelligence is somehow not yet available. This shows that we need to gain skills related to providing real-time data and anomalies. I don't know why it hasn't been done, I have almost reached the point of giving a thesis on this point.

You know, there are City Security Management Systems (KGYS) such as existing skills, biometric data, real-time imaging. But capabilities such as filtering potential threats, making decisions easier, analyzing weaknesses and systematic improvements, security management system can be added.

Another example application, I would like to learn if it is being done in Turkiye. There are Turkish straits, right, like Istanbul and Çanakkale. We make torpedoes, we make sonars, that is, we have sensors related to underwater target detection. So the Turkish straits should have my very competent sonar system so that I can collect signature, propeller, machine noise signature from here. For example, we do not have a system that collects such a signature. Even if there is such a system, there are systems used autonomously underwater, but they are not applied in places like the Aegean, which can be very useful. They can work 24/7 if you put a sensor on them. Americans have systems that work for 6 months in the China Sea. So what is our output from here? We collect data, there is also sensitivity about storing data. So is there a need to store the propeller noise of a dry cargo ship? If no one sees the data in terms of algorithm, we have 2-3 companies that can work. What if we open this data only for certain targets for the development of these algorithms? If the man had money, he would make it himself if he could buy underwater equipment. Also, the university is unaware of the needs. There is also a barrier in the private sector, but it cannot enter because it does not have the infrastructure. Therefore, I think that awareness should be created in order to ensure the use of data by the private sector and the university by sharing it with toy data for algorithm development.

I am skeptical about data confidentiality levels. I think we have a problem with data sharing culture, I think it needs to be improved and this will contribute to developments.

What can be applied in the field for tactical or strategic development? OpenAI has a game solution made with multi-agent reinforcement learning models, tag or hide and seek.

There are two teams here, two teams are playing against each other with multi-agent reinforcement learning (MARL).

In the scenario, agent elements, models, come up with a solution that is defined in the scenario but not thought of by the users. Why am I saying this, the scenario is something we humans cannot see, because the guy tries millions of times, he learns by trial and error in the environment anyway. Is it very smart, no, but it tries 1 million times. If we tried 1 million times, we would find it too. But we have neither the time nor the situation. Therefore, we give it to the model, we learn this from the scenario. So where will human feedback be here? Here it is like this, let's say there is an error in the scenario, or it showed a performance you did not like, or it showed a performance you did not like. You want to add something. There we can give human feedback or we can fix the scenario again.

We were talking about the data process, we analyzed it, decisions will be made. Maybe this will be turned into a strategy, doctrine. Here, let's go over an example from Russia. Now, the places where Russia got stuck in the Ukraine War are clear, it is not progressing despite having 3 times as many soldiers. But if you remember when they attacked Aleppo. At first, news came that they did not have precision bombs in the open source, and it was impossible for them to get out of Aleppo. Then they solved it like this, they destroyed the whole city without using precision bombs. Then what happened? The Russians won there. They also suffered losses in the Grozny issue, but did they succeed, yes, they captured that place. But because they did not analyze why they were successful, they are not in a position to analyze why they were unsuccessful later. There is such a culture here. They established the first secret police organization in the 1500s. They have a strange state tradition. It causes managers to prefer the news they want to receive from the field or bureaucracy to be good, not correct. Then, in fact, data does not come, you do not use a learning structure, data from sensors, intelligence is not important, you do not use it. This is also a problem that I unfortunately see in our exercises. I was constantly seeing the expression that there was 100% success in the exercises. When there is 100% success, there is nothing to solve, we are already successful.

For example, a shallow water destroyer was to be developed in America, more than 30 were to be built, the number was reduced to 3. Why, the project failed. Again, as far

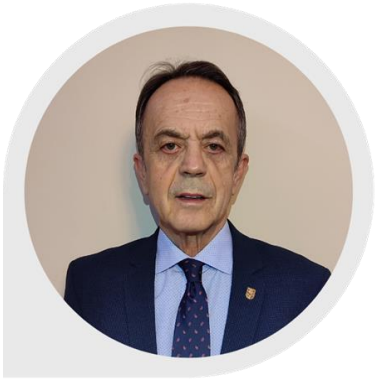
as I read, the 6th Generation Fighter Aircraft development project was also stopped, because it went beyond the budget.

Now there is a situation here, America can fail in R&D projects. I don't know of any R&D projects that failed in our country. But R&D is already a risky thing, it needs to fail at a certain rate. I don't know this dilemma, it seems like there is a problem here.

There are some gaps in the cooperation between university, industry, and the state sector. The training of personnel is done by the state, but there are still some gaps. But the connection there still cannot be established. Because there seem to be some habits, some cultural problems. These need to be resolved so that you can turn the intelligence you collect from the field into a healthy decision and then develop a strategy.

QUESTION: You said security or easy work. Don't these two go together?

ANSWER: Frankly, before the Ergenekon issue fell upon the country in 2009, we could work comfortably anywhere. Then an excessive sensitivity started about intelligence and data leakage and it really reached an extreme point. I mean, I will research an article on the internet, for example, I will research an article on game theory. Now the computers have been separated, closed circuit, now measures have been taken about the internet, closed circuit systems have been established, but. But when something about game theory was searched in a research on the internet computer, the system access was blocked. These may have been overcome, but certain decisions can be made regarding the easier work of the lower level, these should be overcome, this does not seem to be evaluated.



Prof. Dr. Hüseyin BEYAZIT
COLUMBIA UNIVERSITY

Esteemed session chairman and my esteemed commander, esteemed members of the Turkish Armed Forces and esteemed participants, I respectfully salute you all. Since the zakat of knowledge is 100%, I would like to thank those who gave me this opportunity. Engagement, tactical, operational and strategic levels, the lines between them have begun to overlap. Countries like us, in the face of issues such as artificial intelligence and the like, just like the Chinese, we are not reinventing America, we have to develop asymmetric response packages.

I watched a live conference on a YouTube channel by Thomas Barnet, who created the Pentagon's roadmap, and he says, 'In the end, a war will break out between the systems we see, including China, Russia, America, and India, and in 5 seconds, I made it 15 seconds, everyone will blind and paralyze each other.' For this, the Chinese first have the concept of revolution in the military field, which is network-supported, we are saying it wrong, network-empowered capabilities, then network-centric, network static network, network-centric operations, network-centric warfare. He says he will respond to this, instead of putting all reconnaissance, surveillance, intelligence and spy applications into space, I will develop anti-satellite missiles and develop aircraft. Instead of huge nuclear submarines, I will respond to the current conditions with small submarines. I want to emphasize that everyone needs to think about asymmetric response packages.

In 1933, Gazi Mustafa Kemal Atatürk said, 'In our opinion, when evaluating events, we must act according to the concept, the notion of the speed and movement of time.' Then we manage the events, not the events manage us.

We are talking about network-centric warfare in Turkey, defence, information is philosophy and science philosophy. Positive sciences are mathematics. This issue is very important, it does not work when mathematics goes, the basis of all algorithms of artificial intelligence is mathematics. Neurologist

Professor İsmail Hakkı Aydın says, 'Mathematics is the language of the Qur'an, that is, being able to read the universe. I will also present how these are used by foreigners and our neighboring countries that love us very much. Of course, it is physics, chemistry, biology and other sciences such as social sciences. Gödel has a theory; 'There is no problem-free system, nothing in the universe is 100%.' In our tradition of Islam, this is called Sunnatullah.

When we look at an event, we have to look from many different perspectives, that's how the world does it. Otherwise, it's not like what he says, what this says. What does the American say and what does he do? He says mathematics, physics, chemistry. You cannot make these technologies without knowing sciences such as physics, chemistry, biology, you cannot make machines, you cannot fly pilots. Ms. Heidi Shyu, the Deputy Undersecretary of the US Department of defence responsible for research and engineering, said this on April 5, 2023:

«Maintaining competitive advantage is vitally important to educate talented students and individuals. This is only possible with science, mathematics, technology, engineering programs.» Invention, innovation, which they call a very important issue. Former US Chief of Staff Joseph Francis Dunford also said, 'The army that controls the information is the most powerful army in the world'.

What is artificial intelligence? First of all, it is an enabler. It is a National power element, a force multiplier, but it depends on the type and style of operation. It changes the game in combat. It is a game setter, game changer and game breaker. It is a new capability developer, opportunity capability developer for defence, security, intelligence. Just like new operation and combat concepts. It is a capability at strategic, operational and tactical levels. It adds different dimensions to the capabilities and power of defence, security and intelligence institutions. That is, we are facing a new field and a new revolution. What does transformation mean? It means modernization, automation, transformation. What is it in a business world? It means the development of companies for different business models, revenue models and operational, that is, to be able to sustain. What is it in the military? It means new operation and combat concepts, you have to develop very different concepts for each operation type and style. It is also a capacity and an

enabler of new operation, operation, movement comes from, types of styles.

Russian Federation President Vladimir Putin said, 'The one who is a leader in the field of artificial intelligence will rule the world.

Colonel Jon Ercisson, an official from the US Army, said, 'The country that successfully uses artificial intelligence with its army will gain a definite advantage and will also change the character of combat for future generations.' According to some, the nature of combat has also changed, that is, when you look at every type of combat and operation type, the nature, execution, tactics and technical procedures of combat have changed. Its character has changed. In some types of operations, neither its nature nor its character has changed. This is a very important concept to understand how our rivals, modern armies, move. And also the nature and character of combat, when we understand this very well, when we understand the nature and character of combat very well, when we understand modernization transformation and also evolution, then we can easily, flexibly, agilely, quickly and reciprocally create institutions.

US Chief of Staff Mark A. Milley says the following in September 2023; “Continuously developed and equipped with new capabilities, autonomous systems will be much more effective than today's examples in all areas of intelligence and combat, at the command control level and in its execution. In the next 10-15 years, robots will make up one third of the force structure of modern armies. Quantum computers will provide the greatest changes in the fields of defence, security and intelligence.” Look, unmanned is different, autonomous is different. That's how they see it. Look, it's gone, artificial intelligence is finished.

The effects of artificial intelligence technologies on modern defence, security and intelligence are evaluated as the nature, character and execution of intelligence security and combat have changed, some say the character.

Modern defence, security and intelligence institutions are redefining seven critical factors such as a revolutionary new transformation, transformation, namely new operation and combat concepts, institutional structure, doctrine, training, discipline, leadership, education, personnel, facilities. This is the

main force of transformation, the enabler. The transformation is the key enabler of the strategy. Western modern armies, including the People's Republic of China and India, including the Russian Federation, have created autonomous helicopters and autonomous tanks.

While artificial intelligence enables the production of new behaviors and new models in intelligence and combat, it also changes traditional mechanisms that have been used for many years. While artificial intelligence-based smart command control systems help to make quick decisions, they also expand the capacity used in the smart evaluation, analysis, intelligence wheel and take it to more advanced levels. Artificial intelligence develops the data sharing architecture and the operation and use of autonomous systems to more advanced levels by facilitating them.

Artificial intelligence network information systems, unmanned equipment and precision strike munitions, by providing combined and seamless use, intelligence combat cloud, look, technological concepts change the way institutions look at the event, in addition to swarm tactics, swarm intelligence concepts, new smart intelligence and combat theories and doctrines have emerged. The doctrines of strategic level, operational level, tactical and engagement levels are also different.

Dr. John Arquilla from the Postgraduate School summarizes the main goal of all modern defence, security and intelligence institutions in their new transformation strategies as 'quick decision-making superiority for the most appropriate operation style found by artificial intelligence technologies by using cleaned and structured information in Big Data'. I emphatically underline that if you do not structure the information, it will not work, cleaning and structuring are very important. Then it tells you; 'this style of movement is better'. Aviators know John Boyd's 'Observe, Orient, Decide and Act – OODA loop' well. The one who turns this circle fast wins, the one who makes the fastest decision has the greatest competitive advantage. Artificial intelligence is important at this point. The first condition of being prepared for artificial intelligence age conflicts; will be the approach to rethinking the information concept, first of all, not as processing information, but as structuring information. If you cannot do this, you will lose. It is

important that the information is used in all types and styles of movement, that is, the information that is converted into activity, is usable information. Superior information, core information is a force multiplier. Structuring it as information converted into activity is a force multiplier. It is an indispensable condition of intelligence, cyber, electromagnetic, spectrum, space, drones and other combats.

Look, the Chinese People's Army, operation fields will expand from the physical field to the information field, from the information field to the cognitive field. The human brain will be a new battlefield. In 1985, remote mind control was described in America. Zbigniew Brzezinski said this; 'If you give a person 6 dW from a satellite, you become depressed, when you give 8 dW, you become happy.' Even in the early 2000s, at the Armed Forces Academy, there was an electronic warfare aircraft called a commando in America, and this plane went to Canada, this is not a scenario, it was implemented. Imagine we are watching TRT, it enters that frequency and shows you a series. But it makes you, amiably, a monkey, you become depressed, you can't go out. The concept of achieving the target without firing a bullet was discussed in this way years ago, in the 2000s. Subsequently, one of the success criteria in the future will be biological dominance. In my opinion, 'Corona' is definitely a biological weapon. Go talk to doctors and professors. The Chinese woke up, what do they say, biological dominance.

In addition to that, it demands dominance in the cognitive field, as well as intelligence superiority obtained through human-machine interaction. The fields of intelligence have also expanded, the old intelligence paradigm is over. Those who are interested in intelligence will know that they have to develop new doctrines. Unfortunately, this opportunity capability does not exist. A doctrine is an algorithm that tells you how to think. It tells you how to think, not what to do. Look, NATO, in the 2000s, many years ago, was looking at network-centric warfare as a source of power for effect-oriented operations. The physical domain, the domain where combat takes place. Information, which includes information warfare, as well as various dimensions of electronic warfare, psychological warfare, all of which are within psychological information warfare. The cognitive domain and then the social domain.

Let's skip all of them, here what they call human process is also in the literature as influencing how a person thinks in the

cognitive domain, how to make decisions. Influencing how a person thinks in the cognitive domain. What is the new approach to the cognitive domain? Then you cannot create your situational awareness.

The electromagnetic spectrum is a battlefield. Why, look, submarine elements, on the sea surface and on land, in the air, that is, blue homeland, sky homeland, space homeland, cyber homeland and land homeland. All of these are cyber homeland.

Look, in 2020, in the American Joint Vision study, 'communication' is seen as a golden key. A seamless integration, network-centric warfare study is being done. They always looked at it like this and applied it.

And one of the most critical places is 'Cognitive War', what does it say, 'Electromagnetic Spectrum Operations (EMSO) is the heart of operations' it says. Command, control, communication, computer, that is C4 is the heart of war. Look, cognitive world, here commanders, pilots, all have a system. It can be a space platform, it can be another platform. From there they stun our brain, our mind. These are being researched together with IBM and other institutions, being done by forces and countries. The first principle of armies is to seize the electromagnetic spectrum. Because there is no combat without communication.

Ontological warfare, they researched this a lot. Epistemological warfare, algorithmic warfare, cognitive warfare, neocortical warfare, contextualized information, sociological warfare, social media warfare, now social media brigades have reached division level. Public opinion formation warfare and this is according to what the Chinese, Göbel, said; 'The problem within a system cannot be solved from within, there must be external intervention.

Sometimes they look at me like 'What is he saying?', I say 'Unfortunately, you have to listen to people like us, because we look from a different angle. What they call thinking out of the box with very different approaches.' You have to do these, otherwise everything is going very fast. Look at Algorithmic Warfare, what does it say about this? Augmented reality, measurable combat, swarm intelligence and ontological thinking. We have to learn and apply these, these are the things that have been done in the world for years. When we don't know

these, we can't understand friends, brothers, allies. NATO is very interested in these things. Innovative intelligence institutions, the purpose of intelligence, is to strengthen very fast decision-making by turning the intelligence wheel very quickly, reducing complexity, and multiplying the most comprehensive information on the subject. It gives it to decision makers, that's the purpose of intelligence. Military, civilian and have become very close to each other. They even used to say; 'One is a mehter band music, the other is a philharmonic orchestra, they both play together.

The goal is to gain decision-making superiority against the adversary. When you capture decision-making superiority, the matter is over. Artificial intelligence is revolutionizing all stages of the intelligence wheel, all intelligence activities, predictive analysis, cyber security and other issues. It offers tremendous opportunities that strengthen decision-making in intelligence analysis processes and in the preparation and execution of operations. Artificial intelligence is also transforming the fields of global, regional and national intelligence operations. I say outside of combat as well, because fog and friction increase in combat. Friction does not occur without fog, drone combat is very important here. It enables the business processes, current operations and other service functions of large and complex intelligence institutions spread globally and regionally to be managed more effectively and cost-effectively.

As a result of the integration of artificial intelligence into intelligence tasks, the fusion of very large amounts of data from human intelligence, produced by sensor, reconnaissance, surveillance, listening and tracking technologies, and signal intelligence, geometric space intelligence, social intelligence, traditional media intelligence and others, is very important. If we haven't created fusion centers, we're done. We talked about this for the Turkish Ministry of Interior in 2017, for decision support centers, this is very important. Artificial intelligence makes it possible to manage intelligence vision and make determinations about the subject of interest from these data, obtain solutions and make very fast decisions. Artificial intelligence makes intelligence sharing in real time very quickly with artificial intelligence systems. This exists in Iran and Saudi Arabia.

For example, well-known modern intelligence agencies use artificial intelligence in content ranking, prioritized processing,

classification of content features, translation and recording processes to process very large amounts of information coming to their analysts very quickly. The OSIRIS platform, developed by the CIA's Open Source Enterprise and shared with other US intelligence agencies, performs the above-mentioned tasks. The CIA's OSIRIS platform uses artificial intelligence in open source intelligence functions that were based on human experience and labor in previous years. They do the work that a human does in 10 hours in 1 minute.

OSIRIS uses machine learning, deep learning, large language models, multimodal language models, natural language processing models, semantic artificial intelligence, artificial intelligence agents and others to synthesize very large volumes of open source intelligence data and present it for use by quickly passing through those phases of the intelligence wheel. Artificial intelligence-based systems provide result summaries by analyzing and evaluating user contributions through chat bots. For example, in India, Facebook, X and others find that there is an epidemic in the country before the Indian Ministry of Health.

In the very near future of combat, artificial intelligence robots will continue to shape military operations and battlefields with smart drones. Swarm intelligence, drones are shrinking and their use in populated areas is expanding. The new generation air dominance concept and autonomous collaborative combat aircraft are important. In the F35 concept, drones are used as assistants like aircraft for different tasks. Some undertake bombing missions, some are used for signal jamming. Hybrid-hybrid command and control center, autonomous command and control center are very important for the use, management and appropriate use of these technologies. Swarm intelligence is a branch of artificial intelligence and computer-based information computing method.

Swarm intelligence is a branch of artificial intelligence and the Computer-Based Information Computing (computation) method. Swarm intelligence, through the computer-based information computing method alongside artificial intelligence, enables autonomous platforms to use naturalistic algorithms that mimic the movements of living things in nature to solve problems. This technology uses decentralized collective behaviors and self-organizing autonomous systems within

itself. Swarm intelligence is computer-based information processing that uses the principles of biology, inspired by and studying the behaviors and collective intelligence of self-organizing groups in the animal kingdom, such as moving, flying, searching, giving birth, population growth, sheltering and the swarm movements of locusts, insects, bees, birds, fish and others. Members of the drone swarm exhibit intelligent and conscious behavior at the group level by providing unity in effort as a result of their ability to adapt and interact with each other.

All members of the swarm are autonomous and decentralized, meaning there is no central control or Command and control and direct coordination mechanism that dictates how members should behave. The behaviors of the swarm system emerge as a result of the interaction between the swarm members. This makes swarm intelligence systems highly robust and resilient, even if some of the swarm or swarm members leave or are destroyed. The main concept behind swarm intelligence is that the collective intelligence that emerges as a result of the swarm's collective behavior is much greater than the intelligence of any individual in the swarm. This is because the swarm collectively evaluates more options and produces far more solutions than a swarm member finds alone. There are many different algorithms in swarm intelligence that have both advantages and disadvantages. The current problems being tried to be solved are decisive in algorithm selection. Decentralization, self-organization, autonomy and adaptation are four main common points in these algorithms.

Today, the main goal of modern defence, security and intelligence institutions is to rapidly specialize in the field of general artificial intelligence, which has consciousness in it, semantic artificial intelligence and artificial intelligence agents specialized in the field of autonomy in the near future and to increase effective power. In order to achieve the goals in the capabilities of swarm intelligence, they have established cooperation with state institutions, industry, business world, companies, scientists, experts, universities, allied friendly and brother countries to strengthen the invention ecosystem.

The enabler of artificial intelligence is the science of ontology. What is ontology; structured information models. It means ten objects, ton-ness, the being about what the object is. If you cannot establish this, you cannot do anything.

It structures information, it enables the structured representation of information in a field. It is the most important determinant in the adjustment of artificial intelligence technologies and their adaptation to the systems to be used, as it provides 'Structured Standard Methods' that enable the definition, categorization and representation of information. It creates standardized words that clarify the relationship between the concepts that are vitally important in the understanding and execution phases of artificial intelligence, consistent with the user intentions and values of artificial intelligence systems.

It lays the groundwork for 'semantic artificial intelligence focused on understanding the meaning' about data and 'reasoning' data using ontologies. Artificial intelligence agents, which are more than robots, software and simple automation, are autonomous executors who learn, reason, act by making a duty from the situation and make decisions, they have consciousness. Artificial intelligence agents, which are demolition destructors, are the autonomous experts of the very near future.

Today, the biggest problem with this technology is structuring big data. Even if you have the world's best quantum computer, your first job is not to process information, but to structure it. As long as data and information cannot be structured, even if advanced technologies such as advanced artificial intelligence and quantum computers are used, the reality of areas related to concepts, doctrine software, operation planning, situational awareness, situational understanding, common operation picture and comprehensive intelligence picture cannot be clearly represented. The field we want to obtain information about starts with the question 'What kind of reality and phenomenon is it?'. Ontology is both a method that answers this question and a product of this method. In the field we want to obtain information, by structuring the information obtained, it is the discipline of representing, defining, relating and integrating all dimensions, layers and fields of the field we want to represent, what the actors, objects, elements, events, characteristics, processes and relationships are, their structures and types or classes in an integrated way. In the military, 'ontology', which pilots call situational awareness and ground forces call sandboxes, that is, establishing relationships instantly.

How is it used? The American army has been using it in network-centric warfare for at least 20 years. Intelligence ontology, intelligence information ontology, threat assessment ontology, situational assessment ontology, terrorist tracking and surveillance ontology, populated area ontology, space ontology. You cannot track satellites and who is doing what if you cannot establish what all entities are doing. All ontologies used in the space domain, swarm attack ontologies, military planning ontology, bird swarm attack ontology are used in many situations.

So what does ontology bring? It brings a new common approach and perspective, it brings common sense, common language. That is, it serves as a common dictionary for doctrine writers, planners, command level at strategic, operative and tactical levels.

This also forms the basis for creating the common operation picture and comprehensive intelligence picture at strategic, operative and tactical levels and provides this. It offers a common understanding of meaning, again it offers to act with common and controlled terms at strategic operative and tactical levels. It provides common situational awareness and situational understanding, common operation picture and semantic interoperability.

What are our neighbors doing? Aristotle University in Thessaloniki has established an artificial intelligence university with its ontology. A scientist at the University of the Aegean in Mytilene has established an ontology for swarm attacks. What has he done, he has used the knowledge graph of artificial intelligence. After all this information flow, that is, after the ontology was established, he developed a drone product called SARISA SRS-1A, RL275-1S rocket launcher. He placed the world's first drone model using Thales' 70-millimeter rocket, which is launched from a helicopter, on a quadro copter. It uses unguided rockets that have not been developed until now. It offers one or two Hydra 70, 2.75 inch 700 mm diameter rockets with a launch system. It has the ability to hit its target very precisely from a distance of less than one meter or kilometers away. It is remotely controlled and managed by any communication system, including satellite.

Has it finished, it has also developed the long-range kamikaze drone AIHMI AHM-1X. Autonomous ammunition is

dropped from a large drone, UAV or helicopter and can glide for 15 kilometers. After its engine is started from the remote control center, it flies 50 kilometers more at a speed of 140 kilometers, that is, its range increases. It can also use Thales' 70mm and Hydra 700 mm rockets.

Iran announced that it has a technology that shot down an American unmanned aerial vehicle by restructuring its GPS coordinates. The Iranian army announced that all the data on the downed drone was retrieved, the drone was copied by reverse engineering technique, anti-technology was developed against the drone and a new model unmanned aerial vehicle was produced.

Indeed, the biggest challenge for the transformation caused by artificial intelligence technologies is not the technological field, but intellectual and mental obstacles. Human, then ideas, that is, information, content, concepts, doctrines, and then technology. But first human, the foundation is human. An innovative thinking, innovative, inventor and explorer human.

Swarm intelligence needs to be examined very well. A Chinese general says, 'As a result of dependence on each technology, it creates some dark areas in those concepts, doctrines, tactics, combat theory. It is necessary to find and exploit these dark areas. Asymmetric combat packages should be developed by understanding the dimensions of artificial intelligence, algorithms, machine learning and other artificial intelligence technologies. If we cannot understand this, things get difficult and it has tremendous harm to us, it can be. We must work intellectually, understand the weaknesses of technology and develop asymmetric response packages against them.

DAY-2 THIRD SESSION – NEW WAR
THEME:
EFFICIENCY AND SUSTAINABILITIY OF TECHNOLOGICAL TRANSFORMATION

SESSION SUBJECT:
OPERABILITY, SUSTAINABILITY AND INDUSTRIAL DESIGN IN TECHNOLOGICAL MILITARY SYSTEMS

SESSSION THEMES:

Materials science (Adaptable, variable, fit-for purpose, useful, durable design and use)
Ammunition and equipment compatibility
Relevance to real field and technological environment
Autonomous replenishment
Energy and logistics management
SECURITY OF SUPPLY
The complementary equipment ecosystem
MAINTENANCE AND REPAIR

EIGHTH SESSION SUMMARY

The transformation of the Future Soldier concept from individuals to robotic soldiers, the necessity of making 5-10-20 year plans for a technology-intensive battlefield where military doctrines will undergo significant changes with the use of joint technological systems was expressed. While emphasizing the necessity of taking into account the adaptation at the point of speed and endurance in the developed technologies and counter technologies, whether the human will adapt to the machine or the machine to the human in the human-machine harmony process, the importance of carefully following every stage in the development of military capabilities and technologies was emphasized. It was stated that every technology developed today results in munitions, while expressing the importance of the principles of compatibility and hybrid working of old and new equipment in the transformation process of technology, attention was drawn to the advantage brought by interoperability and modularity in terms of capabilities. It was noted that the importance of smart munitions technologies is increasing, and that the production of sensors is a mandatory requirement for developments in this field, while it was stated that investments should be made in all kinds of technical and technological hardware infrastructure for the acquisition, use and sharing of intelligence and operational data. Within the scope of material science used in future military technologies, attention was drawn to the importance of studies on bulletproof, durable materials that minimize injuries, while the need for product diversity in the ballistic protection of individuals and systems was emphasized. It was stated that the production of counter systems that prevent the use and detection of wearable communication technologies and antennas is of great importance in the near and long term, and that projects are needed for measures against these types of technologies, as well as the necessity of studies for the development of high magnetic field generating weapons and laser technologies. It has been emphasized that studies continue for medium and long-range projects in missile technologies, and that domestic production in these categories is of great importance both in the combat environment and in terms of export potential due to the reluctance of other countries to sell.

Air Major General (Retired)
Reha UFUK ER
MODERATOR

Distinguished guests, visitors, welcome. The topics are important, they contain issues that need to be discussed from today in terms of Turkey's future. Before moving on to our topic, I served as both the Air Force Plans and Principles Department and the General Staff General Plans and Principles Department before retiring due to my duty. These studies continue at the tactical and operative levels. However, there is something that is rarely done in our country in general. From that point of view, I would like to briefly remind some issues before the presentations of my guests.

There is a soldier in the middle, we say Future Soldier. I wonder if Future Soldier is a soldier or a point in the nervous system? Should we talk about a soldier, I'm not making a definition, I'm not making a determination, I want to leave a question mark. Is the point we want to reach to give features to this soldier, should we consider Future Soldier as a whole concept? Or is it alive, is it a robot? We have to think about this, are living robots together or separate? On the other hand, will living beings be operators in the back or robots on the front line? While talking about these today, do we have to think about the technologies and concepts of 5-10-20 years from now and the doctrines that will arise from them? Let's examine these a little and continue our inquiries. There are many successful activities in the defence industry ecosystem created today. There are many areas where we can make predictions, I wonder if there are many areas where we make retrospective inferences. I wonder if we can think about the technology-intensive battlefield of 20 years from now and think about the capabilities by making retrospective inferences from there? It is necessary to concentrate on these separately, at one stage I think we should also make inferences about situations where current trends are also part of the problems in eliminating uncertainties about the future.

This is an important point in the steps of future technologies towards the future. A foreign minister made a statement, I leave its evaluation to your appreciation; the cheapest soldier of NATO is the Turkish soldier, it costs 23 cents. I leave it to your appreciation. Should there be living beings or robots on the front lines? Do we deserve this? Let's think about these. 1793, 1944, 2023, look, the years are changing but the order is not changing. Will the next order change? Will there be robots among the soldiers in the military parade units? When we think about speed and endurance, can the two work together? What will Future Fighting Tech, the fighting technologies of the future, be? We need to add the combat intensive technology field to all literature. An example from a foreign organization, which countries are examples of technology intensive war working countries. We do not know how much budget they allocate, but they have allocated budgets. Countries that have established organizations to study and advance this issue have established organizations, they are doing research and development, most importantly they are allocating funds and budgets. The fact that there are countries from Europe to South America, from the Far East to the Balkans on the flags, and that there are countries with different budgets and populations, can also evoke different feelings and thoughts in you.

When we say layers, Future Soldier, is it an aviator, a land soldier, a sailor or are they all within a whole? How should everyone in this layer move in harmony and how should we ensure this unity? How should we define these concepts and how should we establish this organization? In this sense, I would like to thank SASAD very much for bringing such an agenda here. How should we keep them together in harmony and establish the organization? For this purpose, we have established a working group within the Secretariat of defence Industries Academy. We also received the directives of our Secretary of Turkish Defence Industries . We have made it our concern where the technology-intensive battlefield will evolve in the 2040s, which military capabilities, I'm not saying project-technology, military technologies will evolve, and what will come to the fore in the battlefield. We are trying to bring this document into the system within 1 year with STM Think Thank. Beyond these, what I need to say is that organization, budget, structure and concept definitions need to be implemented as soon as possible in order to prevent effort expenditure.

Bülent SEMERCİ
ROKETSAN

Thank you very much, I will make my presentation in two parts.One of the main themes of our session today is ammunition and equipment compatibility. I have prepared a presentation on product diversity and interoperability on this subject. After a brief information sharing about our interoperability and product family approach in the first presentation, I will share information about tactical missile systems.

I will elaborate a little more on what I have described on this subject. Today's changing war environment, the increase in operational diversity, brings with it an increase in the diversity of weapons in our inventory. We assess that when we enter a new operation, it is extremely important that relatively old weapons and ammunition in our inventory work together, are used interchangeably, or are used in a hybrid manner with relatively state-of-the-art weapons and ammunition. What is interoperability? Its general definition is that large complex systems work together in harmony. When you achieve this, we assess that your operational effectiveness will be extremely effective, will increase, and unnecessary resource usage will decrease at that level and your efficiency will increase. We utilize common interfaces of our products and equipment for interoperability. Our tactical missile is an approach based on a product family that allows for operational diversity and is based on interoperability. The two most critical steps of this issue are standardization and modularity. That is, when a new need comes before us from the field, we quickly meet this need with a derivative product approach within the product family and put it into the inventory. In parallel, we can respond very quickly to our customers' demands logistically. We take into account product family integrities in the missiles we develop. We prioritize common architecture, common data paths and common hardware solutions. While doing this, we consider not only our army but also international standards. We do not apply interoperability, modularity and standardization only in weapons and ammunition or launching systems.

We also consider interchangeability, commonality and compatibility within the scope of logistical support. Which logistical support elements? Weapon test equipment, transportation loading systems, training systems, simulators, etc.

I will continue with information about our product families regarding product diversity and interoperability. Our mini smart munition product family, its story started with MAM-L and MAM-C munitions. As of today, this family has a total of 7 members. The system we developed to launch from tactical UAVs can be used from manned unmanned light attack and even jet aircraft as of today. In the coming period, we will also present the hybrid seeker head, artificial intelligence versions to our army's inventory. Our next product variety family is our anti-tank systems product family, which caused the birth of this MAM family. Their births started with OMTAS, UMTAS and CİRİT. We have a history that continues with laser UMTAS and KARAOK. Next year, within the framework of our army's demands, the Laser OMTAS missile, which we call LumtasGM, will enter our army's inventory. As it is known, we developed our anti-tank product family to launch from attack helicopters. But as of today, these 7 products can be launched from a wide variety of manned and unmanned aerial vehicles, naval vehicles and air platforms such as HÜRKUŞ. Our KMC, base-mounted cirit system, is a very good example of product diversity and interoperability. A weapon system that we developed to launch a laser-guided cirit missile can launch two different guidance, four different missile systems as of today. It has really high technology capabilities. Like being able to shoot at a moving target while moving.

Our air systems product family has a story that started with HİSAR and continues with SİPER. Currently, there are 4 products, but in the coming period, we will add 4 more new products here with the SAPAN project. As it is known, we developed our air defence systems to launch from land mobile platforms. With the MİLLAS project initiated by our army's request, we have become able to launch our air defence systems from sea platforms. We experienced the excitement and pride of integrating and launching from different platforms with the launch we made from the TCG Istanbul ship. Within the scope of product diversity, I mentioned Land-Air-Sea systems, but we have also developed products for TEK-ER use.

SUNGUR, KARAOK and METE are these products of ours. We assess that it is very critical to obtain intelligence and operational data in the TEK-ER use concept.

In the future soldier concept, we assess that the single soldier must have a technical, technological hardware infrastructure to acquire, use and share the intelligence and operational data that I said is critical. We assess that it is an absolute necessity for them to transform into a kind of sensor soldier. Although we use these systems for single-soldier use, we will be able to launch them from a wide variety of manned and unmanned platforms, and we are about to finalize the studies for these. KARAOK is one of our most technological products that we put into mass production and gave to the inventory this year. And it is truly a game-changing product in the field. It exceeds 2 kilometers, but we are aiming for better.

Thank you for listening

QUESTION: Do we have an infrastructure for communication in long-range missiles?

ANSWER: Yes, we have and we are working intensively. We think that hybrid seeker heads, beyond visual range and autonomous systems will emerge soon.

Dr. N. Kaan ÇALIŞKAN
TÜBİTAK

I respectfully greet everyone. Under the title of future military, I would like to inform you about material science and engineering applications. First of all, I will give information about the introduction of TÜBİTAK SAGE, and then with 3 main headings. I have been working at TÜBİTAK SAGE for about 21 years.

We have tried to prepare a presentation that includes topics that intersect, separate or contain different evaluations, as we work on the material technologies we have learned in rocket missile technologies as dual use, both civilian and military use areas. We continue our work in an open area of 3 million 100 thousand square meters, a closed area of 75 thousand square meters. We have 1300 employees.

Regarding our mission and vision, our mission is to provide globally competitive and high value-added National technology products and services to the Turkish Armed Forces and the defence Industry through R&D. Our vision is to make Turkiye fully independent with innovative technologies in the defence industry and to be effective on a global scale. Under this mission and vision, we conduct our studies under the umbrella of systems engineering, also benefiting from some areas of expertise. These include battery technologies, guidance control system design, software, material design, various unconventional production technologies, etc. We continue our work under systems engineering. We can list guidance kits, bunker-buster munitions, UAV munitions, cruise missiles, air-to-air, air defence missiles. In fact, our process of transforming into an institution that can make Cirit, one of the main rocket missiles of the Iron Dome, from ramjet-powered air defence missiles at our current position, which started with artillery rockets in 2000, is like this. We have many different products. We have products that are both in the development phase, in the inventory or in production, or that have proven themselves in the war environment. Just as we do system studies, we also have subsystems and products. Because in the products and projects we use, if there is a subsystem that has a

supply problem or cannot be supplied, we definitely develop it ourselves at TÜBİTAK SAGE by combining the necessary expertise.

At the forefront of these are thermal batteries, TÜBİTAK SAGE provides almost all thermal batteries in the defence industry. We also develop sub-components such as pyrotechnic devices, navigation units, antennas, seeker heads, thermobaric explosives and fuzes within TÜBİTAK SAGE. We have a wide product family from electronic hardware, RF hardware, receivers to explosives.

As we made the first domestic National anti-jamming antennas in Turkey, we have also realized the first passive active GPS antenna in TÜBİTAK SAGE infrastructures. While doing these, we benefit from some infrastructures at both system level and sub-system level. Infrastructures that set an example in their fields. Ankara Wind Tunnel, our Environmental Test Center is the largest in Europe, Submarine Tests Infrastructure, Target Ballistics Rail System Dynamic Test Infrastructure (HABRAS), Seeker Head test center, External Load Certification, Non-Destructive Quality Control, Target Ballistics and Ground Tests, Inertial Measurement Laboratory, we have various different infrastructures. Of course, as we use this in our own projects, we also allow our project stakeholders to use our infrastructures. At the same time, we provide services to the armies or related institutions of friendly and allied members in these matters. If there are questions such as what TÜBİTAK SAGE did, did it work, what did it do, you can look at the products obtained from domestic and abroad. Many products of different western origin and used by the Turkish Armed Forces, equivalent or much better products have been developed and used domestically and nationally. We, as its employees, are proud of this.

We can continue with the title of wearable armor technology in material science and applications. I will try to explain how material science and applications, a material science used in a rocket and missile, can be used in a future military concept. Because it is worked and used in developed products through an almost common concept. I would like to start with bulletproof and impact-resistant fabrics first. It is actually a technology used by humanity since the first ages.

Those made with wood, leather, metal and similar materials, then primitive designs used in the war environment. Of course, these are heavy, uncomfortable, products that cannot provide full protection. However, with the development of technology, that is, with the development of production and material technology, new generation vests have been produced and used. Some derivatives and variants in which three-dimensional production methods, which have marked the last 10-15 years, are also used in these technologies. The most commonly used armors are the armors made by impregnating and producing a certain resin, which is more known as the commercial name of kevlar, but technically aramid. It is widely used in the world and can be produced very easily in Turkey. We also have domestic institutions and organizations that can produce very easily with some parts from abroad. However, different fibers other than aramid are also used. These can be polyethylene, polypropylene. These types of materials are also used as bulletproof and impact-resistant fabrics that can be used in different ballistic protections. There are also some studies on ceramic coated fabrics that are being worked on recently, carried out by research centers in the west, and can be worked on domestically and nationally. Studies are also being carried out on this.

Especially, examples in which hardness and abrasion resistance are increased and ballistic protection is increased are also made thanks to this technology. At the same time, different durable fabrics can be produced with different oxide coatings of this aramid, plasma spray coatings. It is also within the scope of these studies that the fabric provides a different ballistic protection by forming a bond and forming a coating surface. Apart from that, after this aramid is produced in epoxy, it is coated with a ceramic such as boron carbide, and durable fabrics are produced by weaving plain weaves or different weaves, or aramid, which we know as aramid, is produced with different resins and different ceramics such as silicon carbide, and ballistic protection studies are being carried out in the world by working on different material parameters. We are also carrying it out. Not only the clothing of military personnel, but also the systems we use have ballistic protection needs. Here, we are also working to transfer our knowledge to fabric technology, and the textile industry is very developed in Turkiye.

It is obvious that good products will emerge when these two technologies are brought closer together.

A new topic is how a polymer called PDMS material, which is very silicone-based, is used in new generation armors and wearable armor technology. These materials are actually flexible materials that can easily take the shape of the body and can be used as buffer material.

However, they have the following features. The moment it is subjected to impact, it changes shape and hardens at a very high level of hardness, acting like an armor, acting like an armor by transmitting little impact to a personnel or the back panel it is responsible for protecting. Currently, there is a method made with kevlar fabrics, but the difference between kevlar fabrics is that after the impact occurs, it protects the personnel by spreading the damage over a wider area while preventing the impact, by distributing the energy, by protecting his body.

The main goal is to minimize the effects that personnel will suffer from the impact by absorbing the impact in a large area as well as preventing the impact. This is used in new material technology, it can be worked with. It is a subject we are also interested in, there are studies on it in some universities in Turkiye and abroad.

Exoskeleton examples are also shown by our domestic companies, by some companies at fairs and seminars. Although the first examples were not very successful in the world, they were later lightened by the change of materials and evolved to carry more loads faster by military personnel working in field conditions. Especially by providing light and strong materials to metal parts, the exoskeleton concept is actually progressing towards success. The exoskeleton concept is also becoming successful by adding new generation materials to the main structural parts with low density and strength ratio.

I will also explain material technologies in nano micro systems as the second topic. Especially the developments in di-electric material technologies, which we have been following in recent years, which we use in RF and electronic hardware,

especially the developments in production technologies, have given us the opportunity to make electronic hardware that can provide different features in very small areas.

Especially, under the concept of electromagnetic directed energy weapon, which is also widely used, concept designs such as electromagnetic pulse generator barrel adapters have actually become feasible thanks to these types of developments. It is very important for soldiers to be able to render UAVs uncontrollable by disrupting their electronic circuits with the electromagnetic past pulse, which we call EMP pulse. Both commercial and military UAVs pose a really big threat. These types of portable and easy-to-integrate designs are actually workable designs in the world right now. When this adapter is removed, the weapon system continues its old function again, providing a convenience.

Apart from that, a very intense activity is being carried out on Nano UAVs. Because military personnel using very small UAVs for intelligence operations have a very great need and requirement in this regard. Although battery life and payload capacity are really limiting factors here, with the developments in material technologies, UAVs lighter than 250 grams, nano UAVs, have been made and can be used easily in intelligence operations. Antenna is actually a subject we are particularly intensely interested in. We can produce all antennas, from anti-jamming antennas to GPS antennas, flight termination, data antennas to telemetry antennas, especially in rocket and missile systems, with our own infrastructures, domestically and nationally, including dielectric materials. Therefore, we work very intensely on antennas. Developments in these new technologies, especially developments in antenna and material technologies, have also facilitated the integration of the antenna into the conditions of the current military personnel. Thanks to chip antennas, different chip antennas, GPS antennas, trackability, health data tracking, cellular communication and facilitating systems are also feasible. Especially the integration into the hand, body or clothing is also easy and simple, sustainable technology with these new technologies. But wearable antennas, which we also use intensively in our own studies, which is another result of this. Wearable antennas are a really interesting topic and a topic that is being worked on by many teams and many academic

groups both in our country and abroad.

Turning the whole body into an antenna by using the human body as a dielectric material after processing it on a fabric with an insulating surface and a pet in a certain texture with a certain pattern. This is actually the basic topic of this concept. Thus, concepts or design criteria, requirements such as tracking health data and tracking the location from the satellite can be easily made possible thanks to this technology. Since we also make antennas with different textures in the antennas we make, we can foresee that these types of technologies can be made by integrating them into the fabric. Developments in the production of small productions with high precision and dielectric materials have actually made comfortable and safe helmet production and design easily feasible. This has made it very easy to integrate components such as head-mounted solar panels, thermal cameras, motion sensors and communication models into helmets. And it has become possible to make it sustainable and work in desired environmental conditions, especially thanks to these developments in material science and production technologies. Apart from this, infrared reflective fabrics, infrared invisibility are already an indispensable concept. Infrared reflective fabric technologies, which will provide this invisibility and also provide thermal comfort, are currently used in the field.

Especially with fabric coating technology in powder, paste and foam form, textiles with different properties in tents, tent cloths or military clothing are produced by weaving. There is no need for infrared invisibility, it can also increase visibility, it also has requirements sometimes. These types of technologies are feasible right now. Apart from that, self-heating canned food technology, which can provide heat without the need for any external source, which uses very simple exothermic reactions, that is, heat-giving reactions, is actually based on a very simple chemical reaction. Studies can be done and used on this. If a simple reaction is used by separating it from food, military personnel can easily use and eat a canned content by increasing the temperature to 30 degrees, 40 degrees, and when necessary, higher temperatures. One of the very hot topics of study right now is wearable heaters.

With the integration of nano thicknesses, by the way, when we say nano, we are always talking about thicknesses below one micron, it is a very important concept to keep the body temperature of military personnel constant in all kinds of environmental conditions. There are studies on this, both in our country and in some studies abroad. Its current disadvantage is that it requires an external source like an external battery. But there are new developments related to this.

Studies to meet energy needs are also important. Since developments in material technologies here have also given us the opportunity to create high magnetic fields in very small units, they are actually leading to the development of new generation weapons in field operations. Systems that can eject penetrating particles at a much higher speed than a bullet, which we call railguns, which work in this high magnetic field, have become accessible with new technologies. There is a possibility that products related to this will come out in the near future. There are also applications in portable solar panels. However, there are requirements related to increasing efficiency. There is also a roadmap towards solar panels where the energy needs of personnel working in field conditions can be easily met by using semiconductor materials such as silicon. Apart from that, thermoelectric material, which we also use intensively and can design and produce, which we call the peltier effect, that is, the use of thermoelectric materials that can generate electricity by taking advantage of the hot-cold situation or generate two different hot-cold areas when electricity is applied, actually offers us widespread and new, innovative solutions. There are many groups working on this both domestically and abroad. Especially the evolution of this into a technology that can provide the electricity needs of the human body temperature by turning it into fabric is currently on the roadmap. Studies will also be carried out on the use of thermoelectric fabric to meet energy needs.

That's all I have to say, thank you for listening to me.

Taylan ERCAN
KALE JET MOTOR (KALE ARGE)

Hello everyone, this is my 27th year in the profession and I have been working on gas turbine engines for 27 years. Today, I have prepared a presentation for you about the engines of cruise missiles. As you know, cruise missiles are very much on the agenda in today's wars. Therefore, we will talk about where we are as a country regarding its engines. My colleagues from both ROKETSAN and TÜBİTAK SAGE briefly mentioned cruise missiles. I will make a presentation about where we are in gas turbine engines, which are indispensable for these missiles. Especially where we are in current technologies, which missiles and engines we have. As Kale Ar-Ge, we have been working on this for about 12 years. Today's concept, namely the Future Soldier concept, the Future Cruise Missile Engine, that is, what we plan to do in the cruise missiles of the future.

As of today, we have 3 domestic and original missile engines, our cruise missile engine. Our KTC 3200 engine is a 3200 newton engine. It powers SOM and ATMACA cruise missiles. KTC 1750, a 1750 newton engine, a smaller engine with approximately half the thrust level, an engine developed for the ÇAKIR platform. KTC 3700 is a developed engine, an upper model of 3200, and 3 different engines we developed for the land ATMACA version. Briefly, if we talk about 3200, it is a 3200 newton engine. It has a specific fuel consumption of .18/kg/hour per Newton of fuel consumption and is a 50 kilogram engine. It is an engine developed for SOM and Turkey's first original turbojet engine. The first member of our engine family, the cruise missile family. Our missile is SOM, at an altitude of 0.6 km, an engine that will provide the propulsion of a missile going at speeds of 0-0.95 mach, and mass production activities are currently ongoing.

The other is our engine that we developed for the KTC 1750 and ÇAKIR missile. It weighs 22.5 kilograms and is half of 3200. This is also the best in its class, of course, starting these works later means designing and putting newer technologies

together into our engines.

Therefore, when we look at rival platforms, having the newest engines gives us the opportunity to develop newer technologies in these engines at the same time. A compact design, high performance and flight tests of all 3 of our engines are also continuing successfully. Our next engine is 3700 and an engine we developed for the land ATMACA version of the ATMACA missile. It is a missile engine with a slightly higher Newton thrust function, similar fuel consumption, similar volume and weight.

So, what will we do in the future, from now on? We have actually reached a point as a country in these missiles and the platforms they are used on, which are actually in the medium range, perhaps ranges below 1000 kilometers. We currently have cruise missiles that make flights of about 45 minutes or less, and their National and original engines. 3200 is actually entering the inventory, in mass production. The other 1750 and 3700 will also be completed their qualifications and given to the forces for use. For the next 10-year period, we have developed these in engine technologies in the first 15 years. For the future, we need to move to a longer range in order to have technologies like those in the world, long range. Therefore, one of its most important components is gas turbine engines. We need to make a move as a technological country here. I have also been working as a part-time faculty member in METU Aviation Engineering since 2013.

Our current technologies, our current missile engines, are actually made with a turbojet architecture, to put it simply. An architecture consisting of a compressor combustion chamber and turbine, to which we give fuel to the combustion chamber and obtain kinetic energy, and we provide thrust by accelerating and ejecting this kinetic energy from the exhaust nozzle. Of course, it is very useful, turbojet engines have been used for years and continue to be used in cruise missiles today. Because it is a simple architecture. But what is the problem? These have thermal efficiency on one side and propulsion efficiency on the other side. Our total efficiency is actually a combination of these two efficiencies.

The main problem with the turbojet architecture is that, in

order to increase thermal efficiency on the upper side, efficiencies ultimately affect fuel consumption. In order for us to increase the range, these gas turbine engines should provide the least possible fuel consumption so that the missiles can travel to higher ranges.

When we want to increase thermal efficiency in turbojet architecture, we need to increase our exit velocity, that is, the exit velocity from the engine or the missile, very much. But this returns to us as a decrease in propulsion efficiency. Because propulsion efficiency also wants to be at a similar level to cruise speed at the most efficiency point. Therefore, thermal efficiency can actually be increased by increasing the engine's own heat up to a certain point and by increasing the pressure ratio inside the engine. But this increase in thermal efficiency returns to us as an increase in exit velocity. Therefore, our propulsion efficiencies tend to decrease. When we think of it as total efficiency, there is a situation that really limits us in terms of fuel consumption. Therefore, when we want to move to long range, for the next generation of future cruise missiles, what we need to do as a country is turbo fan architectures, architectures that we also use in airplanes today.

In turbine engines, we have the same turbojet architecture such as compressor, combustion chamber, turbine, but by adding an extra turbine to the back of this engine and by turning a fan in the front with the power we produce with it, we actually obtain low speeds. Therefore, our propulsion efficiencies become very good and thermal efficiencies can still remain high. Therefore, thermal efficiency is very similar to turbojet, but the total efficiency, which makes the main difference, increases very much. This allows these engines to have a much lower fuel consumption and thus the hourly fuel amount consumed per newton decreases and thus provides long range in missiles. America's AGM series missiles have ranges of 1000-2500 kilometers. Therefore, while missile technologies below 1000 kilometers in the country are entering the inventory in original form with ROKETSAN, SAGE and us, together with their engines, what we aim for in the next 10 years will of course be the development of our cruise missiles in the 1000 and 2500 kilometer range, that is, medium range or long range.

The last topic is foreign sales. There are two important criteria, of course, that our engines are at a similar level to foreign competitors in terms of technology. The fact that we started later as a country means that we can put newer technologies and compete very well with the 10-year, 15-year, 20-year engines in the current market. Therefore, we do not have a problem here. Of course, what else advantage do we have? A cruise missile is also a very problematic issue of intergovernmental sales.

Today, France and America do not sell these missiles anywhere, they do not want to give these technologies. After we develop these technologies as a country, both ROKETSAN sells the missiles abroad, and we sell them more restrictively to allied countries. Therefore, regarding these, especially in the recent period, due to the popularity of cruise missiles and the reluctance of countries such as America and France to sell, we will be selling these missiles abroad for the next 10 years.

QUESTION 1: Welcome back to Turkiye, Professor Taylan. You used to work in the field of Stealth Engine Technologies. Will you continue these studies? Can stealth engines provide added value in cruise missiles?

ANSWER: We are not considering it in the short term, why are we not considering it? Because as you know, we are currently developing the gas turbine engine of our National Combat Aircraft KAAN. KAAN is a 5th generation aircraft and therefore its engine must also have that feature. Our priority target is long-range turbo fan architecture, but immediately after, with the developments in KAAN, we will also be applying stealth engine technology to cruise missiles.

QUESTION 2: We produce engines, we need to produce them nationally. Especially, how much have we been able to localize in sub-components?

ANSWER: We are luckier in cruise missiles, in terms of sophisticated materials. Less technological products. The main difficulties and problems are in GÖKBEY and KAAN engines. There are problems with high sophisticated alloys. Studies are continuing for these. There is no alloy that cannot be produced in specific dimensions in TEI, the necessary technology has been reached from super alloys to alloys that work at high temperatures.

DAY- 2 FORTH SESSION – NEW WARRIOR

THEME:

THE FOUNDADION OF TECHNOLOGY; EDUCATION, TEACHING AND LEARNING

SESSION SUBJECT:

Human-Machine Integration, Education of Human and Technology

SESSION THEMES:

Virtual exercises with AR/XR/VR and simulation applications

Applicable and developmental training programs

Collaboration and adaptation training in hybrid technologies

Continuity of production, maintenance, safety and technology qualified training

Program development based on analysis and data results

NINTH SESSION SUMMARY

In this section, which emphasizes that new technologies require new training methods, attention is drawn to the importance of simulator technologies, augmented reality (AR), mixed reality (XR) and virtual reality (VR) technologies in training. While the awareness-raising and rapid decision-making effect of training given in environments closest to reality is emphasized, it is predicted that scenarios and training quality will also increase with artificial intelligence integration and the concept of digital twins. It was emphasized that the ability of personnel training to make the right intervention at the right time is increased by obtaining biometric data and that their reactions under pressure can be measured. It has been shared that increasing joint operational environments such as air, land, sea, cyber and space in this area will make all military personnel more effectively combat-ready, and that individual training is more possible with these technologies.

It has been noted that applications in which munitions, weapons, and developed systems are tested by simulation provide accurate and efficient product development, which is more important than cost-benefit analysis. The benefits of creating environments where realistic war environments or targets are simulated realistically, where developed weapon and ammunition systems can be tested, and where modeling that ensures correct product development through analyses can be done, and where their effects and deficiencies can be examined were conveyed. Examples were shared that stated that the capabilities of developed military systems can be compared in environments closest to reality and that the use of the most ideal military system is possible with these systems. Concerns about 'false confidence' that simulation systems can create if applied excessively in virtual environments and anxieties about 'perception of reality' that virtual reality can cause were also expressed, and attention was drawn to this dimension in training programs.

In this section, where the international legal dimensions of autonomous systems were also discussed, it was stated that there are many different debates such as the level of autonomy, whether or not there is an operator, the influence and distance of the human in control.

Dr. Oğuz HAMŞİOĞLU
SASAD
MODERATOR

Welcome, our esteemed guests. Thank you for being with us at this late hour when our oxygen is low and the weight is bearing down on us, and for your patience. Thank you for sharing this moment with us. This moment is very precious to us. Because in events like this, the last sessions are always very risky in terms of participation, and we took this risk.

Our topic in this session is education and training, the most important foundation of technology, and the processes in this regard.

In this session, we will discuss machine-human integration, technology and human education in this regard. We will address the issues of excessive technology loading and capacity, user skills, and the concept of cognitive load.

Military simulation will also be on our agenda, and training, hybrid wars, digital wars, information equipment, and personnel-related issues will also be on our agenda. In the lethal technologies section, we will also talk about AR, XR and VR applications. We will address virtual exercises, applicability and developments in mixed technologies, and technology-qualified training topics. We will also make evaluations on the legal issues, especially the human-machine interaction related to artificial intelligence's lethal autonomous systems, and its legal role, as you know there is also an ethical dimension.

Valuable people will share with us. We hosted extremely valuable names in all sessions. And we obtained very good thoughts and opinions from them that will provide a perspective for the future. These will be presented to you as a resource document for both the sector and the user.

Mehmet Onur ÖZÇELİK
HAVELSAN

Thank you. I will start the presentation by talking about HAVELSAN first. Then, I will talk about what HAVELSAN does in Military Training Systems, New Technologies and their impact on warfare, what it does theoretically, what it does in terms of work and products. I will talk about its projects. I will also try to address their impact on training systems, that is, on military training and especially on the field of warfare.

HAVELSAN has been operating in the simulator business for approximately 40 years. About 35-40 years ago, it established a team of 56 people to provide support for the maintenance of foreign-made training systems in the inventory of our armed forces. It has grown with its work and has now become a serious capability in the field of simulators and simulation in Turkiye. What do we do? We build turnkey simulator training centers. Our turnkey means that we establish simulator training centers domestically and abroad with their buildings and training systems. Apart from this, we can offer training systems, which can be platform-specific or different special purpose systems. We have training solutions and products, such as parachute simulators, shooting systems, different special function-specific ones, and civil aviation training systems, an area we have recently entered. We have been in this field for 8 years. Yesterday, we made our first export, and the signing ceremony took place. We exported an Airbus A320 simulator to India. We have significant experience in test and training ranges. One of the business lines we export the most. We have test and training ranges in Pakistan, South Korea, and Saudi Arabia. Live simulation is a serious example of a capability, and we have also carried out projects in decision support and warfare solutions domestically and abroad.

We sell training to pilots from friendly and allied countries in order to utilize the idle time of the simulators we produce domestically. We generate revenue from this and contribute to our armed forces. We provide integrated logistics support services for different training systems that we make or do not

make ourselves.

The new technologies I mentioned here are technologies that you can see in the middle when you do a literature scan. We, as HAVELSAN, are conducting some studies and projects in some of these. The most well-known of these are Augmented Reality (AR), Mixed Reality (XR) and Virtual Reality (VR) technologies. These, especially by modeling the high fidelity level external world environment, provide an environment very close to reality, especially in training systems. These are very helpful in increasing awareness and making quick decisions, especially in training systems. We offer services including conflict simulations and game engines in VR technology to the trained personnel. We demonstrate our capabilities in this field with some products domestically and abroad.

In XR technology, we create an environment where real and virtual elements are actually together. For example, during an exercise, we offer a different environment with a virtual external world in a real cockpit with AR glasses. The technologies here are more theoretical and also new technologies. Like brain-computer interfaces, haptic technologies. Systems that help to understand which stages of which training the stress level of the trained personnel increases by measuring their brain waves and how this stress management can be done. These are now systems that have recently started to be used in training systems. But the hardware to be used for the perception of these waves, that is, brain waves, are very complex and not user-friendly hardware. Therefore, it is difficult to use, not very preferred, but we see it as systems that can be used specifically in the context of personalized adaptable training systems.

Haptic systems can be important to get some sensory feelings, especially in virtual environments. For example, like a conflict simulator or situations that pilots in the cockpit need to feel. These are systems that allow you to feel being hit, touched, or feel a weapon realistically with some clothes you wear on your body. Embedded training systems are now one of the most used systems. Especially simulators, as you know, their fidelity levels can be provided with some certifications.

The training received in a simulator never replaces the

training received on a real platform. Because on a real platform, there is stress involved, some. Especially during wartime, for example, during a dog fight, there are factors that affect your decision-making ability due to some hormones secreted by your body. Therefore, the issue of taking a virtual training on a real platform, that is, embedded training systems, is very popular right now. In this context, we, as HAVELSAN, are trying to develop the embedded training system of both the KAAN aircraft and the HÜRJET aircraft together with TUSAŞ. We will have a surprise presentation at the IDEF fair. The aim here is to see the threats related to this on the screens inside the real platform, for example, if it is an aircraft or a tank, by some forces created in the virtual environment. It can be thought of as the creation of symbologies found in electro-optical systems.

Artificial intelligence is also a technology that is widely used, especially in new generation aircraft. It is indispensable for these training systems. Especially some capabilities such as monitoring performance and artificial intelligence-based enemy elements that can make decisions closer to humans for this performance play an important role in these types of training systems and simulation systems. We generally know digital twin as the digital twin of platforms, but as you know, digital twin is now the transfer of the behaviors and performances of a real system, a system in the world, to the digital world by modeling. This is no longer just on a platform basis, we see it as the adaptation of the digital twin of soldiers or systems, training systems or other systems used to training systems.

Recently, the role of some data collected with real-time data, especially evaluated with artificial intelligence, in training planning is being discussed. Biometric feedback systems are also a very new technology right now. Especially the collection and analysis of soldiers' biometric data in the war environment and training environment. The emergence of a personalized training concept and the implementation of this personalized training by analyzing them with software that also includes artificial intelligence. It has now started to be used a lot. In the past, training systems were standard and everyone was given the same training, the world is now moving away from this concept.

Because everyone's ability, everyone's understanding, everyone's training need is not the same. When you personalize it, you can establish a more effective and more cost-effective training system. For example, a very new term, warfighter digital twin, that is, the digital twin of soldiers. That is, the virtualization of your soldiers in the battlefield in a virtual environment, digital virtualization. You can also monitor this, which is very theoretical in the literature right now. You can monitor the performance of your soldiers, you can plan their abilities in the battlefield or training situations accordingly.

The hologram table called Battle Space, virtual sand table. These are also technologies in the field of training and digitalization of the battlefield, especially with augmented reality and virtual reality glasses in the digital environment. In fact, when you look at the world, there are many applications of this. New training centers are also being established with the latest technologies in our country. Especially in a war time, intervening to a wounded person under so much stress is critical. In this context, making the right intervention at the right time, doing this under very bad conditions, under pressure, under fire, and being able to do these correctly is very, very important. There are systems and training simulations, digital models that measure this. A training center was established for the Turkish Gendarmerie in this context.

Visual augmentation system, especially to increase the situational awareness of our soldiers by reflecting the events that have occurred before in this area on their glasses before conducting an operation in an area. We can also use this in training platforms. Especially what the data to be reflected is can be provided by simulations. This appears as a system that will be used in the real battlefield.

With these technologies, we have done a signal analysis related to heartbeats within the scope of the HRV mental workload measurement project. When you do this signal analysis, you can interpret many things. We did a study with Gendarmerie aviation within this scope. With some sensors placed on their bodies, especially during the mission, what kind of differences they experience, which activity, not only during the mission, but actually which activity within 24 hours causes changes in the heart graph.

We analyzed this with an analysis software and reported what the mental workloads of our pilots are, what their performances, physical performances are. Especially in stressful missions, we presented it as feedback to the commanders. The next step of this was to popularize it in training systems and implement it with smaller wearable technologies.

Genius 2.0 is again a project we are carrying out together with our Secretariat of defence Industries and METU MODSIMMER. A project we are carrying out to measure the cognitive load of the pilot by measuring brain waves and to measure the difficulties experienced during activities, training, which ones cause stress, and what reactions they give, in training systems.

The Five project is a capability like flying with simulators in simulations. But the main important thing is the creation of the tactical environment. That is, the main purpose is to increase the fidelity level in the simulation environment, which includes not only flying with simulators, but also some enemy forces and different forces in that tactical environment. The Five product was a tactical environment software implemented within the scope of the ATAK helicopter simulator, it was rule-based.

It has now been made more intelligent with some artificial intelligence-based techniques. This product is currently used in all simulators in the hands of all our Turkish Armed Forces.

When we say simulation, we actually divide it into three headings in embedded training systems: live, constructive and virtual. We combine these three simulation types in embedded training systems. That is, we run a simulation with virtual entities on a real platform. This also provides feedback by simulating the real war environment to the user by highlighting the physiological effects on the platform and allowing them to be experienced. This system will also be used in KAAN and HÜRJET.

When we look at next generation training concept systems, we see that all platforms such as air defence systems, all smart systems, decision support systems are transformed into an end-to-end concept by connecting to the outside world in a virtual environment with simulators, with a near-realistic terrain infrastructure.

We see that some integrations are now being made accordingly in the world. Platforms are now being integrated with real defence systems, platforms are connected to simulators and integrated.

Training with real platforms that make you feel like you are in a real war by simulating a battlefield is coming to the fore. If it is considered for an aircraft, you provide training capability with the closest virtual environments on a real platform for flight training, shooting and evasion maneuver training in a field with real threats, and situations like dog fights. These are adaptable trainings, they offer the possibility to adapt your training planning as you wish, taking into account the data you receive. Cost-effectiveness offers significant advantages in these systems. With analytical, data-driven results, a infrastructure can be created where you can see the force better with more realistic, better analysis and real data.

Multi domain platform, that is, joint multi-domain control systems, will better reflect the reality of a training environment where not only land elements but also naval and air forces and other elements are together. One of the most important issues here is, of course, being prepared for the real war environment. This is also achieved through training. Especially when you increase the fidelity level and provide this integration end-to-end, it will be possible to make your personnel more effectively combat-ready. When we look at the effects of the war environment, a personnel infrastructure that has experienced the war environment one-on-one with simulations and simulators can be provided at all levels, especially from private to brigade level. Especially making training plans with personalized trainings will become very important for a fully prepared personnel. Recognizing counter forces and the operation environment with comprehensive trainings, creating an atmosphere in the virtual environment that is closest to the environment in that operation before conducting an operation, will affect the result and be more effective.

Orhan Ertuğrul GÜÇLÜ
TÜBİTAK

Hello everyone, our capability that we will present concerns everyone. Because we say National R&D for National defence. Our basic motivation is to offer our capabilities to the sector, especially in the points we see as lacking. In fact, we can say that the fundamental point that S-Force is based on is the simulation of the future and the defence environment of the . future. Let me give an introduction about where we came to this point. TÜBİTAK SAGE has a 50-year history, and actually a very serious history of 25 years on the munitions side.

The fundamental point that our past in the munitions side is based on is our modeling capability 25 years ago. We were established as a guidance control laboratory at METU. In fact, our first studies are based on modeling. We first started with drawings on paper, then with the development of technology, it was transferred to the digital environment. Afterwards, we were able to speed up our process with some analyses. Now let's give an example from an air missile. We are making GÖKTUĞ missile variants, both within visual range and beyond visual range. When we look at these, we come as AIM-120 in our missiles as an equivalent, the certified version of AIM-120 was certified after about 780 shots. 780 missiles were fired. We are closing the first phase of the GÖKTUĞ missile, and at the first point where this closure is based, our simulation past, our modeling simulation past comes.

Our main point here is this. We can close the first phase of the GÖKTUĞ missile with 17-18 shots. So how do we do this? With our capabilities in modeling and simulation. Modeling simulation is very important. Because it is a cost-effective solution, accepted by the world, and a method that will provide them with significant benefits if everyone uses it. Yes, we have training technologies, we have an engineering side, Mr. Mehmet from HAVELSAN also mentioned, especially HAVELSAN's very serious good works. In fact, it paves the way for our country's cost-effective platform system and ammunition development.

This is actually our basic motivation. This is the sole reason we can achieve success with so few sales numbers. Because before that shot, we perform the shots of that ammunition in a real environment, that is, in a digital twin environment of the war environment. We actually trick it and run the algorithms of that ammunition, the algorithms inside that card. By running it, we can see our mistakes there. Of course, we are talking about a very large space, we can narrow it down. But with each shot, we can transfer the accumulated knowledge to the modeling and simulation environment. This is the point where S-Force is based.

There are many capabilities in S-Force. We can use an ammunition in a simulation environment as if we were actually firing it, we have developed an ammunition, we now need some algorithms. Because how many of our cruise missiles, SOM, will we fire at a ship task group right now, how will we fire, from which points will these munitions come, how will these munitions maneuver at the last point when they arrive? These parts are very critical. S-Force is the environment where we can analyze these parts. The name of the environment where we can carry out all our tests in an integrated way is S-Force. We have been using it for many years, at a certain point, certain capabilities are used worldwide, and we are talking about a structure with hundreds, thousands of licenses created. Now let's go into some details, what is S-Force at this point? S-Force stands for Smart Framework for Operational Research Environment. So what are we trying to do here, fundamentally our center is operational analysis. We look at the effectiveness of something, whatever system it is, whatever platform it is, whatever ammunition it is, primarily in the operational field. This is where our fundamental point is based. We create the digital twin of the war environment. Yes, we have simulation environments, we have tactical environment simulators, our munitions fly, hit the target. A decision is made based on the value it hits at the target, for example, the target suffered one unit damage, 50 percent, 70 percent damage. These are not realistic, not a digital twin. What we call digital twin is this, if we really experienced the same situation in a war environment, the destruction at the target, the access to the target, the performance it exhibits while going to the target, are we caught, are we seen by air defence systems while cruising, are we shot down when we are seen?

We need an environment where we can actually analyze this. The two variables on which Operational Research is fundamentally based are Survivability and Lethality. That is, we will first survive, then destroy the target. This is an environment where we can analyze this. When we come to the purpose, we first said the digital twin of the war environment, this is very important, why is it important? The digital twin of the war environment is a very broad concept. What do we digitalize, our impact on the target, the number of our munitions, how many munitions we fired, how many munitions we need to fire, how many SOM missiles should we fire at an Arleigh Burke class destroyer, how many at a single ship, can we hit this ship with SOM? These are very important points. Therefore, this environment needs to be prepared so that we can analyze.

Another point is creating complex scenarios. Complexity is actually the key point here. As you increase the level of complexity, as you increase the complexity, what do you provide? On the one hand, you reach a realistic environment, but on the other hand, you also put forward an environment that is difficult to calculate. This is the point where TÜBİTAK SAGE reflects its experience from previous years. We have a simulation environment, we have modeling capability. In the same environment with different resolutions, sometimes 2 thousand elements can be calculated. In the same environment again, we can perform analysis by running 10-15 platforms on a single computer with very high resolution models. Agent-based tasks are very important. Because you have different elements in the war environment, you cannot manage each one. But you need to define a series of rules for them. For example, I will make this firing if I see it at this point or at this signal level in my air defence system. You have defined this as a rule, put it in the environment, and start an analysis focused on the missile, focused on your platform. What do you do, I fired my missile from this point, it circulated at this point, did it reach the target? You have the ability to create automatic tasks for every kind of element as much as possible with this air defence system, that is. And this is the important point. As we said at the beginning, operational analysis and decision support operational analysis is not just an analysis made after platforms emerge. Concept studies and concept studies within the scope of doctrines are also carried out in these environments.

The theme of the session is the future soldier. So what should the soldier of the future be like? This is also the environment where we will answer the question of what the Future Soldier should be like. That is, what capabilities should they have, on what systems should they be? For example, this is the point where you can analyze all the features you want, such as not being harmed by laser weapons, not being harmed by other weapons, and minimizing the effect of thermobaric weapons. When we look at the point of training and personnel development, the basic point we focus on is that each of our air, land, and sea forces is very strong on its own. You can create a good effect with a single strike here, but the organization of these three forces together is much more important here. We want our current decision-makers to train themselves in this environment on the ability to conduct joint operations, we are preparing this environment. There are certain infrastructures, there are software procured from abroad. But fundamentally, there is a lack of modeling, that is, there is no digital twin of the field. A number of probability definitions are made there, and analyses are made with the definitions made. We cannot see the effect of our current capability. S-Force comes to this point. In the defence Industry, there is a question of what should be in the concept of innovation, the soldier of the future, what kind of war environment awaits us in the future. With S-Force, we are creating an environment where all elements from underwater to space can be modeled.

What kind of environment will it be in the future? Will our satellites be able to remain in space? What will be the effect of our munitions if GPS is cut off? We are targeting a place, we think we will destroy it with 5 munitions, what will happen if we lose our GPS? Are new systems needed? We need to be able to analyze these.

So what are the benefits it will bring? Strategic decision-making ability. Now you are developing a platform. A very important platform, a platform that will determine the future of the country. You say that it should have all technologies, these capabilities, these things. You see that that platform becomes impossible to build. So when will this platform serve? 20 years later. Should these systems really be like this on this platform that will serve 20 years later? Are these capabilities 20 years later? These need to be analyzed. When you analyze these, you put this in front of the decision maker; I will make a platform, my

limits are these. You need to choose a few of these and fill this pool. Especially an important concept for air platform manufacturers.

Operational efficiency, yes, platforms have emerged, we will conduct joint operations or unified operations. In this unified operation, let's say an air strike will be carried out at a point. In this air strike, should the F-16 platform or KAAN go, can we do this with unmanned aerial vehicles? Because cost-effective solution is the most important solution. Look, the best country in this regard is actually England. They do this very well. Especially in World War II, despite having less air power than Germany had, they did not allow the Germans into their airspace. They developed very serious tactics and knew very well at which point to deploy their forces. This is actually the capability we need to have. When we have this, then we are actually very strong individually with the power we have, we have very good platforms in certain platforms, but when we combine this, we need to know what kind of force multiplier emerges.

The cost savings of modeling and simulation are already evident. For this, we have a defence industry company with thousands of employees in our country. We see how effective, how important and how beneficial this technology is. There is also the war environment, we can see the effectiveness of some of our platforms in the war environment. Let's not see the effectiveness in the war environment, let's see it in the digital twin environment, let's see its real effectiveness there, let's develop the algorithms, we will have fewer losses. Fewer unmanned aerial vehicles will crash, less ammunition will be consumed. This is what is important. In terms of security and national defence, our air, land and sea forces are very strong, and when we combine these, we will gain much more than three times the power, there will be a much larger force multiplier. Innovation and platform development is a situation we benefit from a lot. Which munitions should we develop? What kind of environment will it be 20 years later? For example, we talked about GÖKTUĞ missile variants, for example, let me give you a prediction for 20 years later, air defence missiles fired from UAVs will be much more important. Especially from small UAVs, TB2, TB3. This part is very important. How did we get this? Because you can look at the world's trend, you can look at the capabilities of countries. A friendly country of ours buys the F-35 top-level platform, we cannot buy it, we say what will we do.

Whereas 20 years later, there are much, much different scenarios. It is necessary to be able to work on this. This should be our main topic.

We also create some unique scenarios in terms of big data analysis and sustainability. After creating unique scenarios, we create concept scenarios. We send this to batch runs in the background. By changing certain parameters on that scenario, such as the number of missiles owned by the enemy element or the speeds of the missiles or some elements in your defence deployment, you get the conditions of millions of concept scenarios in the background. This actually offers you the opportunity to obtain a large amount of data. Big data and synthetic data, but synthetic data created on digital twin. Very valuable, this also opens a big door for you in the direction of your sustainability.

When S-Force is examined, it has 5 components inside. Sensor, kinematics, tactical environment simulator, new run sides, a structure called sfate that has hundreds of users and thousands of licenses created in the world. By looking at its old capabilities, the models inside are now at a level that can be matched with an intelligence data we have. You can write many tasks, you can do war game concepts.

The important point in a war game is that you can create the war environment as realistically as possible. As long as you can do this, you actually see the correct information. In a dog fight situation, in an air engagement, especially in a within-visual-range engagement, the multitude of your missiles is important. Rather than the speed of your missile, rather than the range, how many missiles you carry is important. You can model all systems, from fixed-wing aircraft to naval elements, in different resolutions. You have 5 parameters to define this platform, you can define it here. The flexibility of the environment also comes from here. You can do analysis by running different elements in the same scenario. Simulator integration can be done. Especially can the pilot engage against an air defence system in a real war environment, how effective is the pilot against it, can he evade the missile fired by the air defence system? You can analyze these. Because there is a realistic environment. There, the model of the platform alone, the system is not enough. The systems on the ground are also very important. How you define them is very important.

How you define them is very important. When developing a platform, it is especially necessary to know the system on the ground. Let's say our missile range is 100 km, its speed is 4 mach, the incoming missile.

You should work at 100-120 km or 4.5 mach speed in order to observe the future environment. S-Force is actually a product range and has multiple products. Basically, the tactical environment simulator, where we create the digital twin, the middle part where we can realistically define the models inside with the information we have in this scene environment is SFate. Under this, detailed sensor modeling. You can define all of them here, optical systems, radar systems, other systems, our sensor means. Kinematics, an important issue and comes from our 30-35 years of modeling capability. You can define platforms in different resolutions here. Air, land, sea vehicle, missiles, etc.

Vision 3D, you have created a scene environment, what does it look like in reality? The user who creates the concept scenario wants to see the realistic scene environment. With the S-Craft product, you can perform millions of runs and stability, sensitivity and trade-off analyzes by changing some variables of the concept scenario. S-Sensor, it has its own radar model or optical system inside. These need to have their own algorithms. There must be image processing algorithms. I developed these in different environments. With S-Sensor, you can fully integrate your algorithms. This allows you to fully test your algorithms.

S-Kinematics allows the guidance algorithms of the models inside to work. If you want to work on some algorithms, you can do that. S-Vision3D allows you to create night vision, infrared images, different images. S-TDL acts as a tactical data link. There are some companies in the world that produce software products of this kind. But there is not a single solution in the world that contains all the systems that a user might need. Tactical data link work is not at a point where it can be delivered to the end user in an integrated way into any simulation product. Here, it can be connected with a tactical data link emulator or a real tactical data link.

S-RT DEVKİT is the section that prevents us from firing 700-800 missiles, which we gave in the GÖKTUĞ missile. Firing 700-800 means 700-800 million dollars. The basis of this is to reveal

the data that those real-time cards created with SRT-DEVKİT need from the outside world. It works in the Linux environment. It works with S-FATE, S-FATE creates the scene environment.

SRT-DEVKİT enables the card to create the data it needs from the outside world by using different simulators such as IMU, GPS simulator that the card needs. S-FTA is our tactical environment simulator, our advanced tactical environment simulator. Smart Frame Work Advanced Tactical Engine is important for us, because the models inside are now at the real level, the digital twin level.

With S-Craft, we can take batch runs. You will do sensitivity, stability, trade-off analyzes in a single scenario. The sensor should be able to be used to define every parameter that the user has as much as possible. This infrastructure is also used with this capability in ASELSAN, TUSAŞ and other environments. It is very important that the parameters can be defined in a way that can make its own system and its own effectiveness. When we come to the radar side, we want to define the antenna, antenna pattern, radar statuses, parameters, PRF value, etc. Because the antenna manufacturer will define these and look at the effectiveness of the system, and even integrate its own model and test its algorithm in a real war environment. Again, when we look at jammer parameters, this is also important. Normally, there are many capabilities in the jammer, systems, capabilities. But when we say jammer, the user will make this DRFM, Repeater, noise jamming, he should be able to define this and also define the parameters related to this.

The kinematics side already has a 25-30 year history. What level of model do I need to create in a 2000 element scenario, what level of model do I need to create, what level of model do I need to run this scenario with, the answer brought by kinematics and 30 years of experience is here. We keep this structure in a collaborative structure for tactical data link. We want to combine our capabilities with companies such as HAVELSAN, MİLSOFT and SİMSOFT. Our main market is not our defense industry here, but our own forces. The main point is to increase its usability abroad. The more it is used abroad, the more data flow and information flow comes to us in some way. When we were using these systems all this time, we were saying, how is this done at point X, how is that done? You are

actually giving some information without realizing it. But when you do this within yourself and make it available to the user abroad, questions start coming to you. This is also a very critical point.

Dr. Osman Gazi GÜÇLÜTÜRK
GALATASARAY UNIVERSITY

Hello. I work as a doctoral member in the field of Information and Technology Law at Galatasaray University Faculty of Law. I study technology, regulation and policies. As you know, law has many different fields. I will mention some issues related to armed conflict law, which I will touch on in a moment, which is actually a unique field. Basically, you see an emphasis on artificial intelligence or an emphasis on human-machine interaction on the screen. The reason for this is actually to connect with the other issues discussed today, but I will also talk about some conceptual reviews from a few conceptual aspects of law. I have a plan during my speech; actually a conceptual explanation, then the importance of artificial intelligence, especially in terms of this concept, for lethal autonomous weapons or Little Autonomous Weapon Systems, which we actually translate from English. And there are evaluations about the legal part of the job and its human oversight, training part, which connects to the other topics in today's session. I want to add a zeroth section here, I will make an introduction like this now. I could have told you here, as a lawyer, that I would tell you how this job cannot be done, based on my experiences in many public institutions, as I think.

But law is not a profession that tells you how a job cannot be done, we see that there is such a tendency, such a prevalence in many sectors. Perhaps it's like this in academia too, but law actually has more than one event. There is an expression that our historiography is quite familiar with; losing what you won with blood with a pen. In fact, the approach in international law exists a little to prevent this from happening. Law, systems in national laws are a little different. There is a central rule-maker, there are some mechanisms that can force you to comply when you do not comply with the rules, that can ensure that you comply. State's enforcement mechanisms, law enforcement forces, etc.

International law is a little different, and when we enter the

defence industry, the matter is that no state, this is not only related to us, this is something that is inherent in the nature of the job, no state wants to bind its own hands and arms, its own defence system, its own national security with its own rules, so we remain in an area that national law does not actually touch much. This has pros and cons, I will mention later that regulations can affect the private sector very badly and ultimately limit the transitions from the private sector to the public and a certain technological development innovation. But the main issue and all the issues we will discuss will be under International Law here. What is done here is actually, in previous sessions, different combat systems and different new types of wars were mentioned. Here, there is a new war and we call this Low Fair, which has evolved into Warfare. The legal struggle in international law actually progresses in the form of 'not what you cannot do, what you can do, but how you do it, you will prevail in that job'. Of course, there are a few obvious examples of this. There are some states that we call the spoiled children of international law, which everyone now refers to in this way. For example, you may be asking yourself, there is such a thing as law, but it does not actually work. Because it cannot affect these states in any way, there are ways to do this.

There are ways to prevail in the confrontation of states, or if something goes wrong, which is generally the case with some professions like law, things only come up if they go wrong, or you deal with them thinking that they will go wrong. It is more unpleasant, that is, when such a thing happens, there are mechanisms that will actually allow you to protect yourself. I will touch on all of these in a moment, now let's get into the content of the presentation without wasting our time.

First of all, there is a concept called lethal autonomous system lethal autonomous weapon systems, and this concept is not a new concept as we think. It is a rather old concept, because the concept of autonomy is actually a concept that we change over time. In a research by Stanford on artificial intelligence, they say something very well expressed, autonomy is a similar concept; 'When we say artificial intelligence, we actually think of a concept that fulfills something that we have not seen until that moment and that we think a human has done until that moment, and we stick the artificial intelligence label on it.

Then this normalizes, spreads, and we stop saying artificial intelligence, then we start saying artificial intelligence to the next new thing.' We actually did this a little in autonomy as well. The line between automation and autonomy really becoming clear, really becoming blurred is a very recent history. Before that, there was actually such a vague line between them, and we didn't really know how to fill its content.

But why is the concept of autonomy important for lawyers? Because we all more or less guess, even if we are not lawyers, that in order for systems, rules to be able to bind a result, to force something on you, it must reveal that you did it knowingly or caused it by not doing what you should have done. We call this a causal link. If there is an autonomous system, an autonomous weapon, and therefore the control of the person controlling it has become very ineffective or cannot intervene sufficiently, then these links can actually break. Therefore, when autonomy is mentioned, when autonomy is said, legal systems are baffled. Because legal systems, whether national or international, are actually based on a certain control mechanism. When you pull this, things get really mixed up, that is, in national laws, there are regimes that we call strict liability, for example, if you establish a nuclear power plant and something happens inside, you are responsible for this. Even if you haven't done anything, even if you have done everything correctly, but state mechanisms work differently. The effect of international law will come into play here. Secondly, it is not very clear what the expression 'lethal' or the expression 'Little' does not cover. Because actually every event is carried to the level of international law, and even to the level of conflict, that is, there is the level of humanitarian law, there is human rights law. If we are talking about a war environment, human rights largely give way to humanitarian law. Because we say that human rights are valid even in a war environment, fundamental rights are protected, but besides this, a brand new and really somewhat chaotic area enters. Armed conflict law and in armed conflict law, some ropes are really broken, both sides are in a situation to harm each other, something will be done, it is not possible to prevent this. And no matter what anyone says, something will happen. We are now trying to minimize the damage, control the parties, and focus on finding a consensus.

Lethal, then we encounter such conceptual effects,

conceptual difficulties in almost every aspect, but the most connected part with today's sessions, new weapons, new war and new soldier is the role of the human mechanism here. That is, how much did we automate the system and when we put what on it, did we leave the human still controllable or not? These will actually need to be examined. There is a definition, the International Committee of the Red Cross (ICRC) and it says, "Lethal autonomous weapon systems are systems that have autonomy in their critical functions, can select targets with activities such as searching, detecting, identifying and tracking without human intervention, and can perform attack steps such as blocking, using force, neutralizing, harming or destroying." They are doing a lot of work in this field internationally and this definition also enters international documents. It talks about "having autonomy in its critical functions and the absence of human intervention." There is such an expression in the definition and it goes on to talk about performing such functions on its own, finding the target, detecting it, perhaps interacting.

Here, it is necessary to separate two things from each other, it has actually been talked about a lot, but this affects our perspective very much in terms of lawyers, and it will also affect a lot in terms of responsibility. It will also affect a lot in terms of the user, operator, and state. In the systems we call support systems, which were also referred to earlier, we do not directly leave the mechanism to the system itself. We give it a place in facilitating some decisions, but we leave the final interaction to human decision. To say that the majority of systems are this is currently the rule of the game. What is happening in the background, what weapons, what techniques are being tried, as we said, it is not always possible to see these. But when you don't do this, you get caught in some regulations and a lot of problems arise that you are taking a lot of risks. When you come to times when millimetric timings, decision mechanisms, and completing that cycle faster can cause much more losses, it is not a very correct approach to come here and say, 'No, we will never allow autonomous mechanisms, it is not possible, we must always keep a human there.

Firstly, your losses can be much greater. Because now, especially with these drones and those much faster, high-level autonomy or high-level remote-controlled vehicles that we see,

which we now consider a conventional part of wars, even the slightest delay or hesitation can have a very heavy impact.

Secondly, when you put a so-called human factor into such a complex structure, it is actually not a very effective and real decision. You say, 'Okay, you will give the final order to fire', but there is a decision support system there. And it tells me, 'Now is the right time or this is the right location, this is the right target'. If you try to make this decision in the simulation world, how effective it is in reality is another matter, because nothing realistic is real, there is a very serious risk there. But asking a human to make this decision in the war itself requires a very serious human resource. This time, to use such amazing weapons with such conventional rules, it means that we need experienced and cold-blooded people whose existence we do not know or whose numbers are very few, which is a very risky investment. A very risky point, so whether we should make the definition, whether we should not, where should we bring the elements in the definition, this is already a separate problem for us.

So what is the prominence of artificial intelligence here? As I said, artificial intelligence is not actually a requirement for autonomy. Because whether the content of the system we call autonomy really needs to make decisions on its own is also debatable. The expressions in the definition are already different. You can include deterministic decision mechanisms under the definition of decision mechanisms with autonomy.

The game of law is a bit like this, that is, it does not play with words, it is already the nature of the profession in law, it can be done. Apart from that, when there is artificial intelligence, the effect of human intervention will change. Therefore, the boundaries of all these things we have talked about will become increasingly blurred and there is one last thing. We will talk about control, we will talk about training, but it is very, very difficult to put this forward and claim that control is really provided.

Because both training processes will change, as I said, and because the system has become complicated, the trained personnel will also need to undergo a new training or their comprehension capacity will need to change. Perhaps you will

need much more people to use a single ammunition or to do a single operation. Because there is a technical side to it. Thirdly, even if you put a person there, as I said before, we do not know what the effect will be.

So where do these take us then? We will go one step further and now we will talk about the law's regulations on weapons, that is, the law's view of these weapons, these systems.

Firstly, why the legal approach is important is important and a separate topic of discussion. There are many risks with autonomous weapons. Many issues are discussed, such as the presence or absence of the operator depending on the level of autonomy, the influence of the human in control, and the distance. But there are good experiments, some of which are thought experiments, some of which are real experiments. The further a human, an operator, is from the conflict environment, the more marginal decisions they can make about human life. This is called alienation. There is a very serious risk of alienation in autonomous systems. Similarly, there is a risk of not being able to see the environment, not being able to influence it, not being able to use information. That is, the whole point of the system is to pull the military, human, and conventional forces from there and move them to another battlefield and gain superiority in the struggle in that way. All of these bring us to different points, different risks, and as I said, we actually see two different approaches in national and international law. Because national laws do not intervene much in these systems because the state does not want to bind its own hands and arms. For example, we have our personal data protection law, but it has a very good Article 28, which explicitly excludes data processing related to national security, this is its nature, this is normal.

There is a regulation on the artificial intelligence system in the European Union that will affect the entire world right now, it has entered into force but has not yet started to be implemented. Of course, it says that applications related to national security, national systems and the defence industry are excluded from this.

Because no one, no state actually wants this. Then what will happen here? International Law will come into play. What kind of structure is International Law? A structure that is signed, a structure that states are parties to. But even if they are not

parties, they are bound by some rules, again, a structure with such strange intermediate nuances, and here we see the most organizations. We see the United Nations, we see NATO, we see the Council of Europe. Now they publish some reports, especially NATO has these serious operational studies. Are situations related to these decision-making mechanisms. We see many additional elements in America's own publications, such as these measures should be taken, you should do these things. But ultimately, can we implement this in the field? This becomes a very important problem. Because there is something that exists in our country, but also exists in international law, setting the rule is one thing, implementing it is another. Therefore, the thing to pay attention to here is, when the event goes to war, since states will ultimately start using force against each other, which is normally prohibited but we cannot say it is impossible, when force is started to be used or when the issue becomes a national security issue, what do you need to do to stay 100 percent safe. It will not be possible for you to remain 100 percent legally compliant anyway. It will not be possible for you to say 100 percent that no one should kill anyone, artificial intelligence should be used very well, everything should be controlled. What should you do to minimize the event, the risk here, what kind of training should we give, what kind of simulations should we do, how should we interact with people, how should we establish personnel, these questions need to be asked.

There is also a separate issue regarding the legal examination of weapons here. Now I will sound like I am saying something new, but this is actually a very old article of an additional protocol originating from the Geneva Convention. Since this was foreseen at that time, international law is not a very rapidly changing system anyway, except for very detailed matters, it is said; 'If you are developing a new system, you will look at these and pay attention to these'. Ultimately, everyone is aware that the event will turn into a bit of jungle law in the content of the law of armed conflicts. Therefore, mechanisms are established accordingly, the introduction of artificial intelligence here poses many risks that need to be considered.

Yes, but what we need to do is still the same, when it comes to that point, to protect the state, to protect national security, to proceed from there with minimum damage in

accordance with humanitarian law principles, some parts of human rights become disabled, in accordance with humanitarian law principles.

So what is the effect of human oversight here then? What did we talk about, in human oversight, the most important thing is a matter called meaningful control. Meaningful control is not just about putting a man in charge. It means giving very serious training, it means showing the field very seriously. But the most talked about thing is reliability, that is, you need to trust this system, the system needs to be a system you can rely on. What does this mean? This system will not turn around and attack your soldier 3 days later, it will not attack you, or you will not lose blood while losing lives and experiencing something bad. In addition, there will be no loss of reputation, and no financial losses.

It is necessary to bring some mechanisms that can pay attention to all of these, and there are important reports and important systems regarding simulation systems here. But simulation systems, for example, the UK example was given, in a parliament session where the UK's regulations on systems using armed artificial intelligence were discussed, there was something very often said; 'You can simulate anything you want, you can never simulate the real environment as it is.' Ultimately, we come to a point where we have to protect both people, which puts an extra burden on them, and conventional systems.

I especially want to say this, a concern that is put forward importantly and I can actually understand it as a period human living at the computer. In case of excessive application of systems and simulation systems, three-dimensional systems and technical environments, virtual environments on a human, that person has both the risk of having a false sense of security and the possibility of their perception of reality being distorted. And when setting up simulation systems, if you do not maintain real-world interactions at the same time, if you make very realistic systems, if you make these very realistic systems, these very realistic systems distort the perception of reality. And there are many studies related to this.

Therefore, we stand in a very strange place. We cannot kill

people, create a real battlefield, kill people and harm, but the technologies we think are the best may not prepare us for reality. We are left in a very dilemma. The only way out of this dilemma is to produce a common solution, to adopt an approach that goes to both sides. Not only to advance technology, but instead to try to both provide training and not reduce the human training contribution in conventional systems. There is a concept of meaningful control, and here, detailed information and contextual mastery regarding the target and the region where the target is located are important.

For example, the issue of predicting the negative situations that may arise if interaction with the target occurs and being able to take measures to reduce the damage that may occur in unexpected situations is important. Situations such as people being continuously actively involved in the process from planning to the end of the interaction and being able to quickly completely stop or at least slow down the interaction will also be important. There is an interesting thing here, if you ask who writes the regulations for artificial intelligence systems, I know them, but I am still surprised that they are written. Among the elements of meaningful control, there is something called effectively shutting down the system. It is like adding a 'kill switch', the red button we see everywhere. I don't find this realistic, I don't find it realistic even as a lawyer. Engineers mostly make fun of these regulations anyway.

Meaningfully terminating the system may cause more harm than good in some cases. Shutting down the system or the system destroying itself before falling into the hands of harmful elements is a completely different matter. But I would like to say that these discussions are important and I think they are going in the wrong direction with some regulations.

I will touch on the training-related part one last time. There are actually multiple things in the importance and effects of training here. I am not a person to preach here, but the person who is harmed, the person who will be harmed, the thing that will be harmed that we are talking about here is the soldier.

Years of effort, training and ultimately national security have been put forward. Therefore, as lawyers, I think that the people who make the regulations, policy makers, law makers are also

experiencing the alienation I mentioned earlier.

Because saying on paper, 'Just don't cause trouble for the state, don't bring trouble to responsibility, pay attention to these' can actually lead to the formation of unenforceable rules in the field. There is only one solution to this, to bring together experts from all fields in the formation of such rules. This is something that is done in some areas, but unfortunately it is not done in some areas. There are important issues regarding the content of the training. Knowing how to use the weapon, which we call the weapon competence system, is one thing, but apart from that, psychological factors are the most discussed, the most criticized and the most difficult to teach topics. Because it was said before without entering that environment, it is really difficult to know its effect. And furthermore, you need people who can know and understand what can go wrong. This is actually a design problem of simulation. When you work in simulation, you act on the assumption that you know all the factors. This is also heavily criticized. What is the solution? I really don't know the solution either. But we also see that the criticism is very appropriate and a lot of work is being done on it. But how it can be solved, what will be done is another problem, I think.

Thank you for listening to me.

QUESTION : In criminal law, there is a provision that says that there must be a mind, which we call criminal capacity, 'the insane cannot be tried.' Like. In the case of artificial intelligence, does a person bring the authority to apply criminal sanctions to a system they have trained? That is, I am the operator, I used it in the chain of command, but the artificial intelligence decision was referenced. What is the result?

ANSWER: Here, I need to separate national and international law again. That is, if this does not turn into an international crisis, if it only remains as an individual internal responsibility event, then there too, our causal link in domestic law, if all the mechanical systems are structured in this way, if all the necessary steps have been taken, that is, these are systems that work with protocols, guides, security mechanisms, locks, they are not left directly exposed.

If this sequence has been applied, if a problem has occurred despite all of them being done, I can say vaguely that a regulation regarding direct personnel responsibility will not arise there. I am talking very vaguely, because there is a small detail in the event, I do not want to fall into a reference like the teacher said. The real problem is in the international law part. Responsibility in international law works from a very different place. There is something we call attribution of a behavior to the state, states are not easily bound, states are bound by their officials, presidents or ministers. Apart from this, for example, if a terrorist organization, a group of people, does something, can this be attributed to the state? There are very serious rules there, it is checked whether the state provided training, provided weapons, condoned this, operated the existing mechanisms that should be operated, or not. Therefore, if training has not been done, if precautions have not been taken, this will also trigger the responsibility of the state. But even if everything is done correctly, there is still something else in international law. Ultimately, you chose to use this from the top of the military mechanisms, responsibility may still arise. This is a developing area right now. Within the scope of international law, serious studies are being carried out in the United Nations in this area. I do not see Turkey's signature in most of the decisions. I do not know whether this is a conscious withdrawal or whether we are not involved. Because we have a representative. But there is a problem in the international law part, we also have rules regarding the resolution of the problem in national law. But if such a thing happens, if you ask about the practice, to be honest, I do not think it can come before the court very much.

I do not want to say something binding, I do not want to fall into the situation of 'you said this' tomorrow, but I am sharing my opinion. Because there are too many confidentiality decisions. I also find this correct by the way. However, some mechanisms will definitely emerge and progress in the future, international investigations will also operate in the future, but that place will experience the result of the military and defence industry being a different area.

DAY-2 FIFTH SESSION– NEW WAR
THEME:
SECURE TECHNOLOGY AND NATIONAL SENSITIVITIES

SESSION THEME:
Privacy, Security and Competition in Technology

SESSION THEMES:

Data Encryption
Cyber Network Security
Information Privacy
Vulnerabilities
Hacker Threats and Backdoor
Electromagnetic Warfare

TENTH SESSION SUMMARY

While it is reminded that technology and satellite-internet infrastructures are at the basis of all kinds of communication today, from people on the street to military units, it was pointed out that the biggest problems could be experienced in communication if cyber warfare methods were applied comprehensively, GSM operators and televisions would be ineffective, and the infrastructure of the mentioned autonomous systems would be affected. While information about intrusions into military systems has been shared since 2013, the importance of cyber security measures was also conveyed on critical issues such as deception, false signals and deceiving artificial intelligence with false data. It was noted that a problem in one link in the chain of military systems that communicate with each other could affect the entire system, and that the risk at every stage, including the processor, hardware, hardware-based vector, supply-maintenance system, should be taken into account in system security.

It was shared with examples that Turkiye's development of its own language model in the field of artificial intelligence requires an approach from a national security perspective, that all kinds of intelligence organizations use artificial intelligence, that it is used effectively in the field of cyber security, and that this issue is handled with a national strategy dimension in countries around the world. In addition to developing domestic artificial intelligence solutions, it was requested that the issue of 'artificial intelligence security strategy' should be addressed as an urgent issue, and that the artificial intelligence security strategy to be created should be urgently integrated into military and intelligence systems' artificial intelligence security. It was shared that audit and security tests should be implemented urgently in the artificial intelligence development process and that cooperation between cyber security companies and research centers should be ensured.

In the session where it was also stated that a 'cyber security' culture should be created in the defence industry and that measures can be taken with very simple applications, an interesting expression was used for the most important difference that separates the war in the field of cyber security

from conventional war: 'The war on the cyber security side is actually over the moment you realize it. Because the person has taken what they wanted, taken it away, or caused the damage they wanted.

Hamdi ERKAN
ASELSAN
MODERATOR

Hello, the last session of this beautiful two-day event has been left to us. The session is the last, but the topic is quite critical. The theme of the session is Secure Technology and National Sensitivities. The concept of secure technology cannot be separated from the concept of the Future Soldier. Secure technology is not just a matter of innovation, it is also a critical responsibility for us to maintain our sovereignty, independence, and social integrity. In this panel, we will listen to important topics such as data encryption, network security, information confidentiality, security vulnerabilities, hacker threats, backdoor vulnerabilities, from experts in the field, both their current situations and their future perspectives. Thank you for your participation, and thank you for your patience in the last session. I hope our panel will be productive.

Regaip KURT
HAVELSAN

Welcome, for two days here, modern technologies, latest technologies have been introduced, especially regarding the implementation of conventional warfare in the field of defence industry. Conventional warfare and the methods and technologies to be used in conventional warfare have been explained.

These technologies will most likely, hopefully we will not see them, but they will be used in a possible war one day, they will be used to protect our country, our nation and our institutions. If there is a war in which we will use these technologies, you will most likely hear about this war from the news. Because it is a total war. But if one day we go into a total cyber war, you will not be able to hear about this from the news. Because the news channels will be unable to serve you, if you want to look at your phone to understand what is going on, you will see that the GSM operator cannot serve you.

Because at that time, cyber attacks have also been carried

out and as a result of these attacks, GSM operators have become unable to serve you.

As cyber security experts working at HAVELSAN, we do not turn to the areas that cyber security experts working in normal private companies turn to. We either produce technologies for use in war conditions or work to ensure the security of military technologies. All the technologies mentioned here, our ships, planes, missiles, software, all of them are put into service by passing through our controls and being verified that they are cyber secure. And their tests are carried out. However, recently, since the penetration tests we do with our classical methods have started to become insufficient, we have started to develop a new doctrine, we have started to develop new methods. These methods include some tools that can be used both in our country and in NATO. Today I will tell you about these tools. Our activities usually consist of continuous red team services and penetration services. These come first. We organize cyber security trainings, prepare CTF and Cyber Range platforms, and actively participate in cyber security exercises in NATO.

Locked Shields is not an exercise within the chain of command, and we were in observer status in CWIX in 2024, this year we will participate as the cyber power of the Turkish Armed Forces as a team. And while we are doing artificial intelligence studies in order to develop the tools we use and advance technology, we are also trying to do something scientifically and practically. We combine these

.

We have a kill chain that we took from military terminology, which we call Cyber Kill Chain. This was developed by Lockheed Martin. And this is a method used in cyber security or cyber attacks. This is a process that starts with the information gathering stage and goes all the way to arming, distribution of that weapon, exploitation of vulnerabilities, and then development of the necessary actions. This process is actually a method used in the military, but in our studies, we developed a new kill chain because we saw that this kill chain was not sufficient in some places. Again, a kill chain taken from military terminology. We have a method we developed called 'Continuous Automated Red Team Service and Penetration Test' that we continuously develop, and there is a difference between this and penetration tests.

When conducting penetration tests, we actually focus on testing system vulnerabilities within a specific time frame. However, because our time is limited, both undiscovered vulnerabilities may remain in that system, and due to this known time interval, for example, if we are testing on the network of an institution, the institution's personnel may take precautions by behaving more strictly than they normally would, knowing that we are there. Since it is a classical approach, the things it can find and show are certain. And it focuses more on known vulnerabilities. It includes the research of 'Zero Day' vulnerabilities, which are unknown until that day, and covers a one-time period. When you test an institution in a one-time period, you can only find the vulnerabilities in that time interval. However, a new vulnerability may emerge one day after that test is completed, and this vulnerability can threaten that institution, these vulnerabilities can have vital consequences.

The things we are going to talk about will generally explain to us how this new war, the new world and the new environment are shaped. However, in the service we call 'Continuous Automated Red Team Service and Penetration Test', we started to provide services to institutions in different ways. We started to do longer-term tests with limited-term or fixed-term agreements. Here, since the time is wide, the possibility of missing vulnerabilities has also decreased a lot. The teams that we call SOC, the blue teams of the institutions, the teams that try to protect the institutions, now have to act more carefully. We have developed a modern approach. Thus, since the SOC teams are also careful here, they have to carefully look at every alarm that comes, because they do not know whether the cyber attack came from us or from somewhere else. Let me give you an example, about 20 days ago we were having a meeting with an institution. In the meetings we held, they said that last year some of their personnel were reached by phone in a certain way and their accounts were accessed, but their senior management did not know that we were there because they received those services, they said that critical data was accessed in another way. At another time, we were the ones who took those data, but they did not know that it was us. That institution's SOC, that is, the blue team, the team responsible for protecting that institution, is always more careful about such things because they do not know it.

We said we are displaying a modern approach and we are also training the blue teams because they do not know these. In this service, zero-day attacks, which are also called zero-day attacks, are tried on the institution's software or systems, that is, if there is a vulnerability that has never been known before in that institution's systems, these vulnerabilities are tested by experts and these unknown vulnerabilities are revealed and this is done continuously. Therefore, since it is not in a specific time frame, we can continue to protect the institution continuously. All military systems work interconnected. Therefore, security must be ensured in all of these military systems.

For security to be ensured, authorization must be done correctly, authentication must be done, encryption must be present and working. Since these are mission-critical systems, they must be continuously operational and they must be resilient in terms of cyber security to protect them. I can give an example from EKDIS on ships, the system that enables the drawing of their maps. Normally, a ship loses contact with the world after opening 10-15 kilometers from land. If it is not connected to a network like TAFICS, if it does not have satellite connection, the ship has no connection with the land. It is a world within itself. The reason I give this example is that you would normally think that you cannot hack a system that is a world within itself and has no connection with the land. The biggest threat to ships in this sense is thought to be GPS attacks. But the maps of the EKDIS system are actually updated from a system that is completely open to the outside world, open to the internet. This may not be valid for military systems, but these types of maps are used in civilian systems and in the vast majority of civilian systems. As a result of the tests we conducted on the FTP server, specifically for these mapping systems, we see that we have access to the system where the ship's map is updated, in a fully authorized way, to change the maps. If the ship updates this system on land and then goes out to sea, since it is completely dependent on that map, it has to rely on this changed map since it cannot update it in the middle of the sea. Even a system that has opened 10-15 kilometers from land and has no connection with the land can be hacked.

I am giving this example because the ship is a very closed system. There is actually no such thing as 'it cannot be hacked'

because it is a military system, it seems very secure. However, some attacks, including military systems, can be affected by some attacks originating from supply chains.

Because sometimes we cannot do 100 percent domestic production, we sometimes have to buy something from outside. These can be processors, hardware, hardware-based vectors. There may be vulnerabilities in them or in other systems. We developed a system taken from the US Air Force. A system we call F2T2EA. There is a saying of Ronald R. Fogleman, a general in the US Air Force, "In the first quarter of the 21st century, it will be possible to find, fix or track and target everything moving on the surface of the world." He developed a doctrine for the Air Force. We also based this doctrine on our new kill chain system. Because if you can find and destroy something moving on the world in less than 10 minutes, you need to be able to find something moving on the internet in less than 10 minutes. If you cannot find it, someone else will definitely find it. Therefore, when providing services to institutions, if there is a vulnerability on the assets of an institution, we want to find it in less than 10 minutes and report that vulnerability to the institution. In some places, there are cyber-intensive and kinetic-intensive conflicts. In some places, cyber attacks were carried out before the armies entered the city, and in some places, cyber attacks were carried out after physical attacks.

So there is a war environment that is completely supportive of the army, physical warfare. This war environment also requires new warriors. The pagers that exploded in Lebanon two months ago could also be done due to a vulnerability originating from the supply chain that I mentioned earlier. If the company that supplies you with the product or software is targeted, a vulnerability may occur that can damage your systems instead of directly targeting you.

There are also 'Advanced Persistent Threat' situations that we call APT, these work in different ways when accessing systems, their motivations are different. 1 For example, we see destructive attacks in Russia's attacks on Ukraine, their methods are usually destructive. 2 State-sponsored hacker groups usually damage the systems they enter, North Korea's state-sponsored groups usually try to withdraw money from the global economic system. Because North Korea's own system is not compatible with the global economic system, it is not suitable for integration. They try to gain the financial support

they lost from here from the other side.

The most dangerous is China. There is something like this on the China side; everything that Chinese state-sponsored groups do progresses in parallel with China's national strategic interests. Therefore, they neither try to cause direct harm to the systems they enter nor do they reveal that they are in the systems. Until China's national goals require them to take a certain course of action or make progress.

There is a group called NSA hackers, Shadow Brokers, they hacked the NSA itself and took some files encrypted and put them on GitHub openly on the internet. At first, no one thought that the NSA could be hacked and data could be obtained from there. But when the password of this file was shared in another deepweb group, it was understood that the files inside were really cyber weapons developed by the NSA and it turned out that the NSA was really hacked. These cyber weapons were cyber weapons that showed that a vulnerability called MS17-010, which would emerge later in 2017, was actually used, this was a system that allowed the NSA to enter all Windows computers in the world. The vulnerability can still remain in some systems, because we do not have the opportunity to update those systems. Because it is critical.

What is NATO doing about this? It is developing a strategy called Active Cyber defence. What we call active cyber defence tells you how to respond to cyber attacks directed at you, in a defensive, proportional, and respectful way to international law. It tries to explain what kind of path you need to follow to respond to these cyber attacks. The part where it says 'Respond don't retribute', the part where it says respond, don't take revenge. What is the difference between the two?

If you are going to take an offensive stance, if only a threat is directed at you, take this offensive stance and make this attack only on the threat directed at you. Otherwise, they say avoid things that will enter the jurisdiction of third countries, that will enter the jurisdiction of third groups. In 2014, at the Wales summit, it was said in Article 5, "If a cyber attack is launched against one of the NATO countries, it will be considered to have been launched against all countries." At the 2014 Wales Summit, NATO said, "If a cyber attack is launched that will cause damage equivalent to a physical weapon, this will now be considered to have been launched against all NATO

countries and precautions will be taken accordingly." In 2016, cyber, space, land, air and sea forces were determined as a conflict area, and studies began here. What we do is actually a combination of what NATO does, what its groups do, or what its groups do, and create an infrastructure for ourselves.

For this, we sometimes do things like target development and preliminary work in NATO exercises. We work on the Locked Shields side on the target development side, the Blue Team side, the Red Team and the Green Team side. There is a reason why we work on the Red Team side in Locked Shields; NATO generally takes a defensive approach. Since it takes a defensive approach, it does not directly look favorably on the development of cyber weapons or the development of offensive tools. But Locked Shields is not a place under NATO's command and control level. Therefore, you can do scientific development, research, software development here. Since we have such an opportunity here, we can develop and use our own Continuous Automated Red Team software here.

On the Cycon side, we are developing a structure called 'AB2F: AI-Based Battlenet Framework for Continuous Red Teaming in Cyber Operation - AB2F: AI Based Combat Network Framework for Continuous Red Team Creation in Cyber Operation'. This also forms the scientific infrastructure of the software of the tools we use in our Continuous Red Team, that is, the framework we use to attack. After these studies are completed, we go to the CWIX (Coalition Warrior Interoperability Exercise) exercise in order to use real environments as an application and testing area and we really do a Read Team exercise there using these software. In fact, things like penetration tests or things done by APT groups can be compared with each other in the context of game theory.

In game theory, there are finite games and infinite games. The characteristic of infinite games is that players try to stay in the game continuously. They are successful as long as they do not leave the game. In finite games, players try to win, they try to achieve something. We, as cyber security experts, especially when trying to protect institutions, are actually inclined to play finite games. Institutions are also inclined to play finite games, but institutions and people who play finite games are doomed to lose in the end, those who play infinite games. In fact, there may be state-sponsored hacker groups, there may be financially motivated hacker groups for financial purposes,

there may be criminal organizations, their only goal is to stay in the game and somehow play that game. Therefore, the structure here can actually be compared to the conflict between states and terrorist organizations. States want to win the game, while terrorist organizations want to stay in the game. Therefore, it is very difficult for a state to be successful against irregular warfare.

The software performs planning and direction, and also carries out attacks in the form of small software pieces as a result of this planning and direction. However, these attacks are not attacks directly defined within the software itself; you need to define these attacks to the software in a specific format. Once this is defined, both information transfer is provided within the team, and when someone leaves, you do not lose that experience, you ensure experience transfer. Secondly, if you can make this transfer, you understand what you are doing much better, grasp it much better, and can move on to the next stage. The software then automates all of these attacks and performs these attacks at certain intervals. After performing the planning and direction, we send a target to what is called the 'Card Workflow Engine' side. It is sufficient for the target you will give to be just a single domain of an institution, there is no need for anything else. After giving this domain, we can extract all assets of that institution that are accessible over the internet. Or, if you have established an internal network, it extracts all the assets one by one in all the places accessible to the software where the software is installed. After extracting these assets, the assets are sent to the slaves after the planning is done. The slaves perform information gathering, and after information gathering, we have our collaboration framework, which is separate software. That software actually processes this information, saves it to databases, and enriches it.

All the assets of an institution, along with the sub-assets of those assets, reside in our databases. Vulnerability analysis and generation are also performed there. I mentioned that we need to find a vulnerability on an institution in less than 10 minutes; because all assets are kept in detail in our database, we detect a new vulnerability in less than 10 minutes and can send information directly to that institution. The somewhat automated part of the work is here; in the analysis and generation parts, the operator and artificial intelligence work together and enrich or repurpose by taking support from

models called LLM. Later, in the distribution and usage part, the incoming data is reprocessed and re-analyzed by enriching it. For this, the method we use is called Black Dagger Black Chart, our software and Lockheed Martin's Software Factory system.

A 3-year agreement is signed with the US Department of defence for this information transfer or acceleration of work. With this agreement, the helmets that need to be produced in 3 years are produced in 1.5 years. Thus, Lockheed Martin is sued for why they gave a 3-year period if they could finish it in 1.5 years. In fact, they see that they can do this in 1.5 years by combining the information from the F16s and establishing the Software Factory system. By integrating this system with our own software, we also ensure that the system works very quickly there. The system here already works completely distributed, it receives IPs from all over the world and has an unlimited IP pool.

The system offers a scalable structure, all tasks work with a user interface and an automation that supports parallel operation. It has an infrastructure necessary for a single task or multiple tasks, and it also provides knowledge accumulation by transferring experiences.

Thank You.

Dr. Celal ERBAY
National Intelligence Academy (MİA)

First of all, we greet everyone who contributed and our participants. In the last two days, especially on the subject of artificial intelligence, very informative and beautiful presentations were made. As you know, especially artificial intelligence technologies are currently under the hegemony of large American companies, but the European Union has announced a new artificial intelligence model that will cover 24 languages. I specifically looked, of course, Turkish is not among these languages, it is a language model in which English largely takes place. From this, we need to come to the point that American companies can feed American intelligence agencies. European developments will feed European intelligence agencies. We can see from this how important it is for us to develop our own language models in the future.

The other speakers also clearly expressed that there is a need in this direction in the presentations made over the past two days. I would like to inform you about what we need to pay attention to while doing this by presenting a similar approach. I will analyze the issue in general terms from a National Security perspective by bringing up the critical role of artificial intelligence in intelligence and security areas.

Distinguished participants, as you know, artificial intelligence has brought about a significant transformation in recent years, especially in the fields of intelligence gathering and national security. This transformation has been rapidly adopted by intelligence agencies such as the CIA and NSI. The CIA, with its investments in artificial intelligence, has demonstrated very significant developments in data processing and intelligence gathering processes. According to documents they wrote, prepared in 1982, I would like to draw your attention to 1982, and declassified in 2012, they have been using artificial intelligence technologies in a key way in their strategic operations since they made their first investments in the field of artificial intelligence. In these reports, they define

artificial intelligence as a teammate. They specifically use Generative Artificial Intelligence technologies to analyze the massive data piles coming from open sources.

The CIA's director of artificial intelligence has stated that these technologies have increased the agency's data analysis speed by 50 percent. Similarly, the NSI actively uses artificial intelligence, especially in areas such as cybersecurity and counter-information. 1 Here, according to artificial intelligence experts, it is stated that it increases the processes of detecting and responding to cyber attacks by 30 percent. The artificial intelligence-based solutions they use enable cyber threats to be detected and prevented at earlier stages. The NSI also actively uses artificial intelligence technologies to monitor election security and disinformation campaigns by foreign actors.

When we come to China, they have placed artificial intelligence at the center of their national security strategies, using this technology in a very wide range from cybersecurity to military operations. According to the new generation artificial intelligence development plan they published in 2017, they aim to become the world's largest artificial intelligence center by 2030. According to this plan, artificial intelligence shows that it will be a critical technology not only for their own economic development but also for national security. One of the most striking points here is that China, like the NSI, uses it in the field of cybersecurity. The Chinese Intelligence Agency, namely the Minister of State Security (MSS), uses artificial intelligence to detect cyber attacks early, protect data from manipulation, and respond quickly to threats.

They also widely use their developed artificial intelligence-based facial recognition systems to ensure public safety and quickly identify potential threats. As it is stated in open sources, I will also express that, especially in the building where consulates are located in Beijing, with artificial intelligence systems integrated into cameras, or rather, by analyzing the employees working in the consulates, a CIA group was exposed, which is seen in open sources. This actually shows us the point China has reached. They also use it very actively in military operations outside of the intelligence agency.

The People's Liberation Army of China is developing

artificial intelligence-supported weapon systems, and these systems are actively used to direct target detection and attacks more accurately and quickly.

Artificial intelligence has brought great innovations to attack methods in the field of cybersecurity, greatly increasing their effectiveness. By accelerating artificial intelligence-based hacking attack processes, here again I want to underline, it allows even individuals with low technical knowledge to carry out effective attacks. Artificial intelligence attacks take place in stages such as reconnaissance, gaining access, impact and data theft, privilege escalation and lateral movement, and evasion of defences. The first stage is the reconnaissance stage, where attackers gather information about the target system; artificial intelligence can present very valuable data to attackers by scanning open sources and various platforms on the internet very quickly. It is actively used especially to identify personal information, email addresses, and security vulnerabilities.

The second stage is the access stage, where artificial intelligence creates fake emails and messages with methods such as phishing, and can easily access sensitive data such as passwords and credentials by deceiving users with fake content. Again, artificial intelligence-supported deepfake technologies help target individuals pass identity verifications by producing fake video and audio content. The third stage is the privilege escalation stage, where attackers use artificial intelligence tools to gain more authority in the system by using the access they have obtained. Here, artificial intelligence generates the necessary commands and directions. Thus, attackers can easily move deeply in the system. The fourth stage, the impact stage, can make attacks such as ransomware especially faster and more effective. Artificial intelligence technologies can encrypt files and deliver ransom demands to a wider audience. Finally, evasion of defences. This is also quite critical, as you know. In such systems, artificial intelligence tools create polymorphic malware that constantly transforms itself to prevent the detection of malware, and this helps attackers easily evade cybersecurity systems. Some of the artificial intelligence tools used in this sense are software such as WormGPT, FraudGPT, Poison FPT, AutoGPT, FreedomGPT, ChaosGPT, White Rabbit NeoAI.

You can find more artificial intelligence tools as you research. For example, WormGPT allows such attackers to create unlimited content and makes it possible for them to evade security filters. Again, software such as AutoGPT and FreedomGPT help cyber attackers in these processes. For example, FraudGPT can produce fake pages, malware, and cyber attack tools for cyber crimes. Such tools are accessible to software through certain Telegram channels. That is, it is not distributed in a very public way. Especially in the area we call deepfake, the area we call the deep web, such tools are made available. In general, such tools allow hackers to manipulate targets, produce malware, and carry out cyber attacks more quickly and effectively.

As we have seen with examples, artificial intelligence models are now of quite critical importance, and it will be the same for our country. And frankly, perhaps such an artificial intelligence model should first be developed in the fields of defence Industry and Intelligence. And we must be very careful during the development phase of this. The artificial intelligence life cycle consists of development, deployment, design, and maintenance stages and sub-components. We have to be very careful at every stage of this, and I want to show how potential risks and vulnerabilities that may occur at every stage of this cycle can be exploited.

During the design phase, which is the first stage of the artificial intelligence life cycle, the lack of a security architecture can cause attackers to inject malicious data into the system. This, what we call poisoning data, can be used to give false information to artificial intelligence during the training process, and this can affect the results. This can lead to very serious consequences such as erroneous intelligence reports in military and intelligence systems, failure of military operations, or manipulation of surveillance data in our future use. The second stage is the development stage, where security vulnerabilities can arise. Continuous monitoring of systems and insecure code writing, inadequate access controls, and poorly configured models at this stage can allow attackers to manipulate the system. The third stage is the deployment stage.

Here, too, security vulnerabilities can arise. Insecure API endpoints, misconfigurations in cloud services, and inadequate

encryption can lead to manipulation and attacks in artificial intelligence application environments. Especially in systems like unmanned aerial vehicles, if there are such vulnerabilities, attackers can change their navigation routes or take control of the systems. The last stage is the maintenance stage. Here, there is also a critical process in terms of security. Systems need to be continuously monitored and updated. Again, security patches, necessary security patches need to be applied in a timely manner.

Especially in cybersecurity applications, neglecting the maintenance of artificial intelligence-supported defence systems can make the systems more vulnerable to attacks. To summarize, artificial intelligence security vulnerabilities can lead to different threats at every stage of the life cycle. In the process of creating an artificial intelligence model, all these vulnerabilities in the artificial intelligence life cycle are fundamental elements that both security experts and technology developers should pay attention to.

If we are going to develop an artificial intelligence model in our country, which is a very critical and urgent issue, especially after the recent developments. I would like to summarize what we should pay attention to. At the core of our country, I want to emphasize its importance again, it is necessary to develop domestic artificial intelligence technologies, this is quite an issue. Domestic solutions are very important to reduce foreign dependency in the field of artificial intelligence. Domestic artificial intelligence solutions are one of the most important items that will allow us to keep security under control here.

Again, I would especially like to emphasize that the integration of domestic artificial intelligence solutions in Turkiye's defence industry will reduce the national security gap and create a more robust defence capacity. Again, Turkiye's artificial intelligence security strategy, we know we have a roadmap on artificial intelligence, we have a roadmap on cyber security, we actually need to create an artificial intelligence security strategy as well. If you are going to develop such a language model, creating an intelligence security strategy is

also of great importance. And if we are going to create this security strategy, we should start by integrating military and intelligence systems with artificial intelligence security. Artificial intelligence can accelerate many studies and provide great benefits in critical tasks such as big data analysis, cyber defence, and counter-terrorism in the military and intelligence fields. However, of course, it is important that these systems are designed securely from the beginning and that security protocols are implemented from the very beginning. Another important issue is the explainable artificial intelligence issue. This technology needs to be invested in. One of the biggest security vulnerabilities encountered in artificial intelligence systems is the lack of transparency in decision-making processes. Therefore, as Turkey, we should ensure that the artificial intelligence to be used in our national security systems is explainable. In this way, by transparently revealing how artificial intelligence systems work and with what data they make decisions, we increase the accuracy of artificial intelligence.

Finally, continuous audits and security tests should be carried out on artificial intelligence systems. This should also be one of the important items of our strategy. At this point, it is important to increase the resilience of artificial intelligence by cooperating with cybersecurity companies and research centers operating in our country, with penetration tests and continuous monitoring systems.

To summarize, artificial intelligence offers very important opportunities in the field of national security, but these opportunities also bring some risks. 1 Leading intelligence agencies in the world, such as the CIA, NSI, and MSS, have quickly adapted to this transformation. They have been actively using artificial intelligence for many years. 2 The European Union has also taken a serious step in this direction, and frankly, it is our turn to quickly bring these issues to the forefront with such a language model and use them in the military and intelligence fields. I would like to conclude my presentation by stating that artificial intelligence technologies require strong policies and strategies from today to be prepared for the security threats of the future.

Best Regards.

Bülent ARSAL
STM

Thank you very much. First of all, I would like to thank you all individually. It is the last presentation of the panel. But I will talk about both my own experiences and what can be done simply but effectively, what are the methods. In fact, I will be talking about cybersecurity exercises at its core. In the previous panel, information about simulation environments was given. We will be talking about the situation on the cybersecurity side of this.

I have been working in the defence industry for about 2.5 years. Previously, I served as the head of USOM within the Information and Communication Technologies Authority (BTK). That was entirely focused on telecommunications, communication, and completely on cybersecurity. This side is entirely the defence industry. I have noticed that cybersecurity in the defence industry lags a bit, its priority is a bit behind. We are doing really important things, we have UAVs, we have ships, we have planes. These all have a physical counterpart for all of us, they are generally made as systems and are not as open to the outside as possible. They recognize friend and foe, they are designed accordingly, and cybersecurity lags a bit behind. However, as we all follow, normal IT systems, which can include software, simulation, and applications, are now very close to production in the defence industry. As a matter of fact, there are people at the core of all of them.

I have been working in cybersecurity for 20 years, and 20 years ago the biggest problem I encountered was passwords. From the first day I arrived, it was passwords, and if you look now, the biggest problem is still passwords. Now imagine if I gave someone the passwords, when I get hold of an admin's password, I'm actually doing a very big job. That is, I want to say that if we can actually add cybersecurity to our lives as a culture with some simple applications, we can very easily get rid of most attacks. Now, there is a very big difference between defence security and actually cyber warfare, that is, cyberspace called the 5th Dimension and the war on the

cybersecurity side, which is described as a battlefield, and normal conventional warfare.

That is, the war on the cybersecurity side is over the moment you realize it. Because the person has taken and taken what they wanted. You don't even realize it, but in conventional warfare, there is even a declaration, I have declared war on that country. Or a missile is sent, it is clearly clear that the war has started. But this is not possible in the cybersecurity world. If you have noticed, at the very least, your own phone, computer, when you notice a movement there, you know that someone has entered there. Maybe they stole and took the information, it's too late. You now try to detect this. Apart from this, there is another important difference.

In the previous session, law was mentioned, international law was mentioned on the law side. War, cyber warfare, Chinese APT groups, Russian, North and Iranian hackers were mentioned. But these can never be proven, which systems they did it with, when they did it, how they did it is absolutely not clear. That is, there were definitely those who explained it themselves, for example, Israel explained this regarding pagers. But it is very difficult to find any retrospective trace of its evidence. Because these are very complex attacks involving many components. Therefore, there is a very big difference between them.

The dynamics on the cybersecurity side are very different. If you look at the cybersecurity side as you would in normal conventional warfare, like in the defence industry, we are actually one step behind. There is a very easy way to solve this, I will say exercises, but it is debatable whether enough importance is given to them. What are the steps, types, scenarios, teams, domestic and international exercises. There is actually the STM Cyber Range service. My aim is to simplify the work a little bit. As I said before, password is actually a very simple concept for all of us. But it causes very big things. Here, exercises are actually not given much importance in appearance. Except for the exercises I attended, except for Locked Shields, they are generally seen as an angarya job, so to speak. However, whether it is at the table or operational exercises, these affect our working culture, our workplace culture and the culture in the defence industry. And as long as

we gain this culture, I think we can be a little more successful in this regard.

Now, when we look at the military exercises, what does it actually bring us? It brings us a culture, both individually within ourselves, as an institution, as a whole company and actually as a whole country. It changes our perspective. What are the steps? These first start with planning, everything will ultimately start with planning. Here, what kind of exercise will I do? Because the field of cybersecurity covers a very wide area. There are OT systems, systems in the defence industry, IT systems, cloud systems, artificial intelligence. A planning is needed on this side. Here, keeping the scope too complex may not add anything to us; we prepare scenarios suitable for the methods, starting with a more focused scope that will bring something to everyone as much as possible. Then, we actually put the military exercises into practice. We start whatever is in the process scenarios related to this, we make the attacks, we fight each other. Subsequently, a report emerges as a result of this, and within the scope of this report, I now extract what is strong and what is weak on my side and make a report. I provide training to develop my weak points or to further develop my strong points. In fact, it's very simple, maybe I compare it to this.

The European Cyber Resilience Act was published in Europe. This will also come into force in the European Union. There are a total of 12-13 items there and it actually says; for all digital element-containing products, it is divided into two parts there. It covers every product containing digital elements, and there are 12-13 basic items in them. These are actually very simple items that we all know. What are they? For example, it says do your updates, it says systems should not contain known vulnerabilities. These are precautions that we should normally take in our daily lives. It is very easy to implement. But it is necessary to ensure its continuity for you and for it to enter our lives as a business. As I said a little while ago, if an attack is learned, it is too late. We must be constantly vigilant not to encounter this. People working on the cybersecurity side know that if things are going well under normal conditions, if the systems are working, maybe the names of the cybersecurity personnel are not even known. But if there is a problem, if a system is cut off or an attack has been defeated, then the

person responsible for cybersecurity is called first. And it is learned there who it is. This is actually one of the methods to prevent this. We need to add this to our internal functioning, both as an institutional culture and as our own lives.

Cybersecurity has three basic elements: confidentiality, accessibility, integrity. But on the exercise side, there are people, processes, and technology. We have very detailed systems and software, but we are lacking in the process and people part. In the defence industry, as I have experienced, we have too many processes, these processes are written down and followed, attempts are made to follow them. But on the other hand, there are not as many processes in the public sector or the private sector. You may have followed it recently, Russia is remotely carrying out a wireless attack on an institution in America. How does it do this? First, it attacks an institution and companies that can be in the wireless network area close to that institution, takes them over, and from that computer, it attacks the other side because it is included in the other side's wireless network. Therefore, it is not very logical to say that 'my wireless network cannot be attacked from here, Russia cannot come here this way, what will happen here' by just saying wireless network. The same applies to the defence industry, we all use computers, internal and external networks, but there are points where they merge. Stuxnet is an example of this shown years ago. None of us have a guarantee that it is not happening now. The other third difference is that we have no guarantee that attacks on the cybersecurity side are happening now. We cannot say whether it is happening at this minute, or we cannot say whether we are attacking. Maybe 6 months pass, a year passes, the attacker has finished his job and left, then he makes his voice heard.

If we continue with the types of military exercises, there are technical simulations, completely specific to the application, specific to the relevant institution, specific to the defence industry, specific to sectors such as energy and health. These are prepared by using more of the systems, technical devices, and software there, and they follow and control more of the human skills and processes there. They reveal the current situation of both institutions and individuals. What kind of process do I run during, when, and after a cyber attack? How does my personnel there react? How can I get out of here with

the least damage? The other is a table-top theoretical military exercises. This is actually an military exercises that completely shows whether our processes are working properly.

Table-top theoretical exercises are often somewhat disregarded. We can categorize the scenarios into three types: There are scenarios with network infrastructure. IT/OT, cloud network architecture, phishing, active directory attacks, internal and external threats, monitoring and detection, network security, and DDoS attacks.

Completely need-oriented military exercises can be conducted. If you remember, one of the world's largest DDoS attacks was an attack on DNS infrastructures. Even systems like Amazon and Twitter were damaged. There are parts related to malware. You can think of one side as hardware. There are attacks related to ransomware, command and control center, bot software, malware analysis, keylogger, trojan, webshell, or application security vulnerabilities and exploits, which we all know. One of the most important is those related to cybersecurity vulnerabilities and exploits. Because we have too many systems, we use too much technology, and it is not easy to keep track of whether they are really up-to-date, whether there are vulnerabilities here, whether they have been patched. For this, it is appropriate to conduct serious military drills.

Another important part is scenarios related to management processes. When an incident occurs, there may be legal repercussions, either from abroad or domestically. If there is a data breach notification related to KVKK, we must have a processing process. There are scenarios related to preventing attacks with threat intelligence, to be able to detect whether an attack is happening or not in time. Communication channels are a separate issue, because they need to be transferred to the relevant places in an appropriate way to avoid reputation loss. There are military exercises teams. The red team is the part that uses all kinds of methods to attack and capture. The side that uses everything it knows, saying 'everything is permissible in war'. The blue team is the part that tries to defend completely at the point of 'Çanakkale Geçilmez', tries to take all kinds of measures, and does all the analysis. That is, they mutually measure their own capabilities here and also try to measure the institution's resilience in that regard. There are domestic and international military exercises.

NATO conducts regular exercises every year. 1 The most important is Locked Shields, coordinated by the NATO Cyber Command. Many public institutions and private sector support are provided here. Similarly, support is also provided to the NATO side. Domestic exercises have a separate importance. They are organized by USOM, domestic exercises are different for different sectors, separate for the financial sector, the energy sector, and there are simultaneous military exercises with foreign countries. The difference here is that the attacking team is usually USOM itself, and the others try to defend a system made for them.

The point I want to emphasize here is that we can actually prevent most cyber attacks with some simple measures, and the importance of taking the necessary precautions in the cybersecurity world, which has a really different dynamism.

We have also started a Cyber Range service at STM. Here we have four different sections. We have a very simple academy section, a scenario section, a laboratory section, and a Cyber Range area. Our aim is to fully increase the training, personnel quality and competence of the relevant institution, company, companies in the defence side in their own academy side. It takes place in three different stages, beginners, intermediate and advanced. And they are followed and guided. The other is scenarios. There are scenarios that can develop scenarios and allow the person to think like an attacker, like a hacker, gain their perspective, and be competent. These are current and engaging practical scenarios suitable for different competency levels. There are laboratories, we may want to specialize in a subject. For example, you may want to specialize in a device on a product side in the defence industry. From there, we create a laboratory related to it and create a section there that will provide competence in this subject to the end. The other is the Cyber Range area, we actually have a system where we combine all the academy, scenarios and laboratories, bring them together, bring the red and blue teams together and watch their mutual struggle. Thus, with the Cyber Range side, we aim to increase the competencies of all companies, all institutions, Turkish Armed Forces, and the defence industry in the cybersecurity field, which has a different dynamism in the cybersecurity field. At least in the cybersecurity side, we wish to see the least damage in events such as the pager incident and the attacks we have

experienced recently, to take the necessary precautions by detecting them as early as possible and to take the necessary security measures before reaching this point. Because the main important part of cybersecurity is not the part where I will not be hacked, but we need to work to increase our effectiveness on this side with an approach of how can I detect this as soon as possible, how can I see the least damage. As STM, we are trying to provide all kinds of services for this.

Thank you.

Çağlar AKMAN - HAVELSAN - CENGAVER PRESENTATION

Hello, I will explain HAVELSAN's CENGAVER, the military concept of the future, with a live demo.

Firstly, I will explain what Digital Unity means. After going through the steps of what kind of needs a future soldier has, I will tell you what HAVELSAN understands by the concept of a future soldier and what it offers you with the name CENGAVER, and then we will do our real demo.

When we start with the Digital Unity concept, the first thing to be understood is actually 'an integrated smart integrated network'. The situations that start with sensors and networks in this network, each sensor is no longer a cognitive entity from static sensors placed left and right, but wearable sensors on us or a unit that can perceive the environment on robotic technology, which has a structure that allows to perceive the environment, not heterogeneous sensors, but also has actuators, and can intervene in the environment. The definition I just made remained on the engineering side, it did not have military jargon. When we say Digital Unity, the 'Digital Unity' concept emerges when we combine the traditional military competencies, strategy, and traditional military perspective into the architectural structure I just created.

We can divide it into four hierarchical blocks. ADHOC network is indispensable for this. Because it consists of mobile units, ranging from independent small groups that make decisions on their own in the field to large battalions, and there are autonomous systems that support these in addition to human units. Next, our soldier deployed to the field, you can call it 'Digital Soldier, Future Soldier or Dismounted Soldier'.

Autonomous vehicles, unmanned aerial, land, and sea vehicles form the third part, and the technologies that enable the formation of a situational awareness picture form the fourth part. The digital soldier concept takes all these features as a digital unity. In fact, the most advanced unit here is a unit where traditional military tactics are combined with technology. What is planned to be done here is to enable the soldier to make more effective and efficient decisions by increasing their own effectiveness and situational awareness.

For all these needs, the name of our product that reflects HAVELSAN's vision is 'CENGAVER.' Now we will continue our presentation on a real CENGAVER soldier. Smart watch where you can get health and activity data, location, headgear and glasses that provide real-time image streaming support, communication headset and microphone, wearable sensors and processors, tactical and portable DOOB system designed with the main goal of increasing situational awareness, can be added.

We are talking about establishing a system solution where refined information reaches him with the complex technological units he carries on him, enabling him to perceive what is happening around him, and share the information he produces with his friends or other team members within the team.

Let's move on to the title of what the needs and requirements of a digital soldier might be. First, environmental sensors. There are shooting detection sensors that can detect threats such as area, CBRN, that are placed around, placed around, that can detect threats around. These examples can be diversified and this is part of the digital soldier. Here, we need to add the sensor solution of the appropriate team with wearable technologies, in accordance with the operational concept. Considering the fact that more data can be transmitted from one center to another very quickly with the development of

battery and wireless communication technology, and that wearable technology has also developed, you can see that it is part of the digital soldier.

It's not a situation where sensors will be hanging from everywhere like a tree ornament. It's not about abundance, it's about scarcity, the necessity of obtaining maximum situational awareness information with the least amount of material is one of our most important goals. In these first two stages, we do not turn to a solution that the user does not want to wear, which is an unmanageable complex. We aim to share the data with both a team and the center in an appropriate bandwidth for effective communication.

By interactively combining this information with the autonomous devices that are the concept of the digital unity, being able to receive simultaneous information, ultimately a decision support will emerge. As HAVELSAN, we are trying to provide decision support and situational awareness picture from the tactical field to the operational and strategic level by integrating our products such as the command and control system we developed with the name HARBİYE, and the DOOB product tree through the system.

The last component can be summarized as cybersecurity in addition to physical security. We can handle this with the products developed by HAVELSAN like lego, like a puzzle. Like, delete the part you want, add a new one or the necessary one. The thing to remember is that we cannot load weight on the personnel that they cannot carry.

It's not just about weight, we can have demands such as not exceeding 30 kilos, working for 72 hours, working for 36 hours. This is not enough; we say this way because we talk through measurable metrics when end-users and engineers come together. We can define it as a requirement, but we need to remember that humans will use it at the end of the day. Our goal is 'motility' which has 'movement force and ability', not 'mobility' which means 'mobility'. That is, not to hinder mobility. It should not be uncomfortable from any sensor on his arm or leg, it should not hinder his flexibility of movement. Therefore, any desired feature can be added, but we must produce a product that is need-oriented and does not disrupt his peace, comfort, and especially the efficiency of his operation.

Firstly, the indispensable backbone of the digital unity is

communication. Our goal here can be likened to the answer to the question we ask for our children, for example, 'where are you, how are you, are you okay?' After we turn the human into a sensor, we connect them to a communication network, a network, with a communication network.

Traditionally, GPS works outdoors, but when we enter closed environments, there were ready-made solutions related to Bluetooth and Wi-Fi from the past. As HAVELSAN, in our software and protocols where we received 8 patents last year, we have an 8 patent ultra-wideband-based relative positioning solution. We can perform precise positioning in both previously entered and previously unentered environments. We reach this information with the 'where are you' answer from the watch. In addition to information such as heart rate, blood oxygen level, and temperature level found in children, whether they are running, walking, fainted, fell forward, fell to the right, whether there is an unexpected increase in heart rhythm in their body. This is not a clinical watch, this is a health watch. I must reiterate that the desired information and the increase of information depend on the number of sensors to be placed.

So what did we do with the information we collected? Let's explain it with our demo. The soldier in the field can have a cell phone or a tablet, we have software that can show his own situation, the situation of those around him, and the situation of threats through the interface. At the end of the day, if this soldier were in the field, he would only have a radio and a watch. If the commander wants more information, he can also have glasses for image transmission to the remote headquarters. As if there were a table in the middle, the commander can follow the location of all personnel in the field in real time, follow their health status, and obtain images and data combined with autonomous working systems with the camera on him. The reality and proximity to reality of the data will be supported by graphics containing augmented reality and mixed reality. Meanwhile, the drone can follow the key team member. The drone can follow him from a certain angle.

QUESTION: Our soldier on the stage is young. For example, a soldier born in 2000 would have been born using Windows software, while the commander wearing virtual glasses is 40-50 years old, and the one he will take orders from is perhaps older. Here we are talking about three different generations, such as X, Y and Z generations. We are talking about different generation

technologies such as Android, DOS, Virtual glasses. How will this generation gap be overcome in these technologies? Also, your presentation was software-focused, on the hardware side there is the IVAS project, which the US started, canceled and reopened.

What are your suggestions for the most important issue here: the production of durable hardware suitable for electronic warfare and combat environments, and its high-volume production?

ANSWER: I constantly emphasized sensors, obtained information, engineers, and end-users. Our intention is not to say, 'we do these things, we can do them'? We cannot teach tactical and traditional military tactics, they will teach us. Our goal is not to give them new toys either. We come with techniques that will provide the information and hardware we know they need. Otherwise, we could have put as many different sensors as we wanted, added small projects, and dazzled. We could have made a more colorful presentation. That's why we explained with simple questions, with sentences like 'where are you' and 'how are you'. Will this system be installed on all soldiers? It cannot be installed everywhere, it can perhaps be installed on special forces, special operations, personnel whose training and cost are difficult. So, was the military lacking because these technologies did not exist now? No, it wasn't, I mean, was there much more trouble before these? No.

We are saying here that you are already getting these needs with radio and correspondence. We are speeding this up. We are also giving you an assistant cognitively. The assistant will not try to teach the commander command or write new doctrines. We are showing what can be done with technologies, he can read it again in writing if he wants. Does it have to be glasses? No. The way of collecting valuable and known useful information from the field will not change, we are speeding it up. The defence industry did not teach situational awareness to the soldier, the soldier taught the situational awareness ontology to the defence industry. We comply with them. We are also presenting how to make the things we have learned from them and the things they have drawn the boundaries of more usable with technology.

As for hardware, would you buy a phone without software? We cannot put the software somewhere without hardware either. Hardware is important, but without software, applications, functionalities, hardware is also worthless. The hardware production part is established in the world. Very large investments are also needed for the useful design of hardware. We do not reference hardware in any way. As HAVELSAN, we have patented algorithms and software. Companies A, B, C, D, and E can also produce hardware suitable for these tasks, we say we can integrate the software. HAVELSAN's great vision is to focus on software and algorithms. CENGAVER is aimed to be developed as a 'system of systems' where technologies are added at every stage, where tasks and authorities are defined from a single soldier to the highest-level decision-maker in the Command and Control concept, where strategic planning is done, where a communication infrastructure is provided to enable plans to be transmitted to the tactical and single soldier level, and situational awareness is provided at all levels. It provides superiority over its counterparts with its number of sensors, real-time data transmission and positioning features.

ADDITIONAL TECHNICAL EXPLANATIONS ON QUESTIONS:

- If the system lacks topographic or map information, it will provide positional information in initially entered environments. We use technologies that provide instant mapping for cave-like environments with lidar and different sensors. We obtain operational health data, not clinical, regarding health.

- Operational health data, not clinical health, takes precedence in health and fitness-related data. However, the scope of this data can be expanded.

- All kinds of features, data transfer, and characteristics can be changed according to the demands of decision-makers, whether at the Battalion, Brigade, or soldier level.

- We recently completed a European Union project. We delivered it in Brussels in June 2024. Within the scope of Digital Unity, we delivered similar systems to high-level officials and special soldiers.


HAVELSAN


ASGER
HAVELSAN
HAVELSAN

CLOSING STATEMENT

Semih DEMİRTOKA – HAVELSAN

Dear participants, our valued guests,

During our two-day Future Soldier event, extremely valuable panels were held here, valuable information was shared. I also had the opportunity to contribute as a panelist in the Hybrid Technologies and Multi-Domain Operations panel. We had the chance and opportunity to share our views and receive good questions from you. The soldier and technologies of the future were discussed within the framework of New World, New War and New Warrior. In the previous panel, a reference was made to the management of this change transformation. In fact, while the subject of the soldier of the future is technological, we need to change our mentality, continuously, innovative or so-called disruptive, to use a trendy term, we need to constantly seek how to improve in so-called disruptive issues. In that sense, I find this conference valuable in this context. You are all defence industry employees or enthusiasts here, in the defence industry, there is competitiveness in other sectors as well, but what keeps us excited and alive in our sector, I think, is that you develop a measure, the other side develops a countermeasure, you need to take a measure against its countermeasure. Therefore, you are in a constant race, you are in a high-speed flowing river, you are trying to survive. Even more importantly, you are trying to be a leader. Therefore, in this context, I find this Future Soldier conference valuable.

Actually, our SASAD Vice Chairman of the Board and HAVELSAN General Manager Mr. Mehmet Akif NACAR was going to attend the closing speech. But we achieved HAVELSAN's first civil simulator export success in India, he went to India to sign the contract related to it. Since he could not make it here, he sent me. I thank you again for your participation.

Looking forward to seeing you at the next event, have a good one.

EVALUATION AND CONCLUSION SECTION

EVALUATION

FUTURE SOLDIER TECHNOLOGIES AND INDUSTRY PERSPECTIVES

ARTIFICIAL INTELLIGENCE RECOMMENDATIONS

CONCLUSION

EVALUATION

- The use of artificial intelligence in military systems and technologies will increase.

- While it is presented that the fundamental tool of artificial intelligence and what it is truly best at is its ability to break down data and analyze it, it has been stated that its greatest contribution in our lives and in the military in the current period should be considered as analytics facilitator-centered. It is recommended that preparations for the near future, when artificial intelligence is still taking its first steps today and its true reality will be felt, be accelerated.

- It has been reminded that information operations and destruction through information operations are the oldest strategies in wars and that their methods have changed throughout the historical process, and artificial intelligence has also been defined as a scalable and measurable last generation information operation tool.
- There is a common view that communication, command and control, communication computers, intelligence, reconnaissance, surveillance and target detection capabilities will be the first target of artificial intelligence applications in the future war environment.
- It is predicted that artificial intelligence will transform the productivity of defense and change military capabilities in the near future with strategy development, regulation, and completion processes.
- It is thought that countries such as China, Russia, India, and America will prioritize the use of artificial intelligence technologies in autonomous and robotic technologies, especially in the field of autonomous swarms and electronic warfare. Artificial intelligence is expected to play a significant role in military and strategic competition.
- It is thought that artificial intelligence-supported military capabilities will increase the impact of technological military capabilities by increasing speed, location, and lethality.
- The fact that America can fly a jet with an artificial intelligence algorithm and perform 8 different tasks autonomously has been defined as what artificial intelligence can do at its birth stage. It was shared that due to artificial intelligence working faster than the human brain, it is necessary to construct well how we can integrate the autonomy growing with this type of technology into industry and human resources.
- It is recommended to show interest in every developing technology with the principle that "falling behind in a technology developed by the adversary opens the way for possible disasters.

- It is foreseen that artificial intelligence can be tested on self-learning and interpreting military systems in the near future. And it is noted that it has begun to be trained to understand and react to hostile behavior.
- The use of artificial intelligence is seen as a factor that will determine the degree of information superiority.
- It should also be kept in mind that artificial intelligence is about imitating the given data, making interpretations from the data instead of finding something original. Therefore, until the training processes where artificial intelligence will fully yield results, methods to be developed with algorithms that provide control and optimization are also recommended. It is thought that giving importance to the development of human feedback options that will make decisions or make recommendations will contribute to critical decisions and work efficiency. In this direction, software, projects and studies can be prioritized in the process of artificial intelligence development.
- It is thought that blockchain technology will provide a secure data infrastructure by combining with quantum technologies in big data processes."
- Cyber attacks can be the source of doctrines that will affect wars as the perfect integration of the digital and physical world.
- Quantum communication technologies will be the encryption system that will determine the difference and make systems secure in the near future. Developing measures on this issue as well as adaptation should be among the priority issues.
- Quantum sensors, biotechnology and nanotechnology fields will rapidly develop. Future projections and investments in this direction are needed.
- The impact of unmanned aerial vehicles and autonomous aircraft on air superiority will continue to increase.
- Artificial intelligence-supported autonomous task completion capabilities are described as a factor that will provide a significant advantage against electronic warfare.

- It is necessary to be the developer and technology leader in all technologies, including artificial intelligence. Especially in critical technologies, investment should be encouraged with common cooperation models.
- While unmanned land and sea vehicles and robot dogs are considered the first signs of small robot wars on battlefields, it is predicted that medium and large robots will take the field, first as logistics and then as active combat personnel, in the 10-20 year period.
- Autonomous air, land, and sea vehicles moving in swarms will begin to be much more effective on battlefields in the near future. It is thought that integrated operation concepts of autonomous military technologies and traditional war technologies will be tested for a while longer in real fields with artificial conflicts.
- It is predicted that the importance of low orbit satellites will increase. The tasks undertaken by Elon Musk's Starlink satellite technologies in the conflict between Russia and Ukraine support this prediction. It is thought that space competition and wars may begin in the near future in near orbit, lunar and earth orbit.
- It is stated that the development of defense systems for systems that work using them, as well as reconnaissance, surveillance, intelligence and spy satellites, and studies aimed at gaining electronic warfare capabilities for missiles will gain importance.
- Jamming systems and target deception systems will gain a different dimension with artificial intelligence. The digital twin concept is foreseen as an electronic manipulation method among the important war doctrines of the electronic warfare field.
- There is a need for the development of technologies that prevent detection by the enemy and new products in this field, as well as vehicles and systems that affect maneuverability and logistics in the field.

- Generating visuals that will increase situational awareness from the analysis results obtained from big data will contribute to the processes during operations and training.

EVALUATION

- Studies on integrating systems that regulate body temperature, provide protection against infrared rays, use low energy for the technical devices they will use, and generate energy from movement and environmental factors are being carried out extensively worldwide in the clothing of the TEK-ER.

- System integrations for contributing to soldiers' load carrying, endurance, strength and mobility with exoskeleton systems are gaining importance.

- It is recommended to give importance to clothing and technology studies that will prevent the soldier from being targeted or minimize the damage by eliminating possible threats, in addition to communication and intelligence.

- Even if you have the best systems, you cannot guarantee the result if you cannot determine what to use when. The brain and talented people will not lose their influence for a long time, despite all technological developments.

- It is predicted that technological developments will restrict the physical movement activities of soldiers all over the world and that new types of ailments that develop with technology may occur.

- It is recommended that personnel who will use especially autonomous and robotic systems and work at the desk, who will command such technologies that require long-term attention, be subjected to new generation training programs psychologically and physiologically.

- The reaction speed of personnel working in the field with technological equipment or mobile loads in critical situations should be one of the special examination topics. In addition, studies on technology production and use are recommended in terms of force, speed and endurance balance.

- The armor developed by the Russians to protect their tanks against drones using techniques dating back to the Assyrian period is regarded as an indication that the old can be renewed with the new and of the place of the human mind in war.

- It is recommended not to completely abandon traditional warfare methods, anticipating possible disruptions in technology, and to be cautious in this regard. The combination of traditional methods and developing technologies is considered the most important aspect of the development period of war technologies.

- People or companies that catch up with current technologies will play an important role in wars as proxy actors. The positions of companies like Starlink, X, Facebook, and Microsoft in the Ukraine-Russia war are considered indications of this.

- The importance of simulation systems in increasing awareness and making quick decisions in training is increasing. In particular, exercises in near-realistic war environments accelerate the adaptation processes to new technologies.

- It is expected that the next version of deepfake and social media wars will progress to the mind-reading phase, where emotions and feelings are also analyzed and added to the results. It is expected that social media software, VR glasses and technologies such as neuralink will increase the role they play in conventional warfare and prepare the ground for this process.

- Attention is drawn to the necessity for companies, military units, and organizations to go to new structures for the effective use of artificial intelligence and new generation war technologies. It has been stated that rapid work is required, especially in the field of training and trained personnel.

- A period is beginning where it is more difficult to predict which reality of the enemy we will have to deal with in the future. War and conflict environments are foreseen where very fast reactions will be required in too many dynamics.

- Analysis is considered the most important element of individual and technology development. At this point, while the capabilities, performance, limits, and development of personnel and the technology offered are accepted as the basis, there is a need for an analysis-centered approach and production style in all processes.

- In all matters such as cyber security, hybrid warfare, unmanned land and sea vehicles and autonomous systems, simulation, virtual reality, competence in intelligence, analytical skills, psychological resilience, fast and accurate decision-making, and human management also have the potential to gain force multiplier status.

- It is stated that human capability as well as the technical infrastructure to process, evaluate, and make decisions on the data to be delivered by a large number of different autonomous or computer-based systems will be needed.

FUTURE SOLDIER TECHNOLOGIES AND INDUSTRY PERSPECTIVES

317 BILLION $

41 companies in the US-based Top 100 recorded $317 billion in arms revenue. This figure represents half of the Top 100's total arms revenue and is 2.5 percent more than in 2022. Since 2018, 30 of the first 41 US companies in the Top 100 increased their arms revenue in 2023.

133 BILLION $

The total arms revenue of the 27 Europe-based Top 100 companies (excluding Russia) reached $133 billion in 2023. This was only 0.2 percent more than in 2022 and represented the smallest increase among world regions.

103 BILLION $

The nine China-based Top 100 companies saw their smallest annual percentage increase in arms revenue (+0.7%) since 2019, amidst a slowing economy. Their total arms revenue in 2023 reached $103 billion.

6,7 BILLION $

The total arms revenue of the three Indian companies in the Top 100 increased by 5.8% to $6.7 billion.

2,2 BILLION $

The UK Atomic Weapons Establishment (AWE), which designs, manufactures, and maintains nuclear warheads, recorded the largest annual percentage increase in arms revenue (+16%) among UK companies in the Top 100, reaching $2.2 billion.

sipri

2 December 2024

ARTIFICIAL INTELLIGENCE SUGGESTIONS

"Investing in the defence industry in Türkiye is strategically important and an area with growth potential. Considering global trends and Türkiye's current defence industry infrastructure, you can focus on the following areas:

Unmanned aerial vehicles (UAVs), unmanned sea vehicles (USVs), and unmanned ground vehicles (UGVs) are now fundamental elements of modern armies. With the increase in autonomy levels, the demand for unmanned systems is growing rapidly.

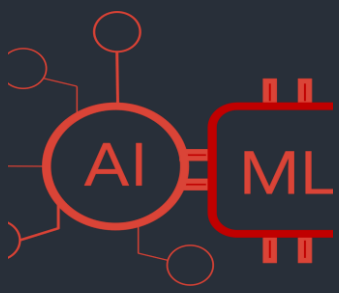
Artificial intelligence (AI), sensor fusion, and big data analytics are critical to increasing operational effectiveness and accelerating decision-making processes. Wars are no longer fought only on the physical battlefield but also in the cyber environment. Protecting critical infrastructures and attack detection and prevention systems are of great importance.

Laser weapons are seen as the technology of the future due to their ability to provide precise intervention to targets and low-cost ammunition. Durable, lightweight, and low-cost materials are critical for both military equipment and armor systems."

FUTURE SOLDIER TECHNOLOGIES AND INDUSTRY PERSPECTIVES

According to Deloitte's 2025 forecast released on October 23rd, the impact of expenditures made by 59 countries due to the war situation in 2022 is expected to continue in 2025, and many technologies, from artificial intelligence and advanced air mobility (AAM) to unmanned systems, have the potential to become widely operational. Over the past year, artificial intelligence has seemingly become ubiquitous, indicating that companies in the sector are becoming increasingly comfortable with the technology. In 2025, artificial intelligence is likely to help accelerate progress in various areas, such as improving after-sales services and optimizing the supply chain.

The revival in air travel over the past year has significantly increased the demand for new aircraft. As aviation and defence companies face supply chain quality challenges and declining fleet availability, the call to extend the operational life of existing commercial aircraft is growing. One way to extend the operational life of aircraft is through effective maintenance, repair, and overhaul (MRO). Therefore, companies are identifying value opportunities, such as integrating digital technologies to meet the need for greater efficiency and cost-effectiveness, with advanced MRO services.



According to a recent Deloitte survey, 81% of respondents from the aerospace and defence industry reported that they are already using or planning to use artificial intelligence and machine learning (AI/ML) technology. Responses from after-sales companies also indicated that AI/ML, generative AI, and augmented reality are the main focus technologies for the next one to three years.

Deloitte.

FUTURE SOLDIER TECHNOLOGIES AND INDUSTRY PERSPECTIVES

According to the US-based Space Foundation, the global space economy reached US$570 billion in 2023, representing a 7.4% increase over the previous year (in line with the projected five-year compound annual growth rate of 7.3%), mainly driven by the commercial sector. In particular, the positioning, navigation, and timing (PNT) sub-sector accounted for approximately 47% ($209 billion) of the commercial total of $445 billion. This market is expected to grow by 155% by 2035 and may be a major focus in the coming year. Companies across sectors, from supply chain management to transportation, are likely to continue to rely on PNT technologies for location-based services.

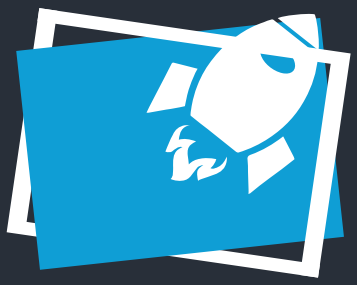
The US fiscal year 2025 defence budget request reflects the focus of the United States Department of defence (DoD) to continue investing in strategic areas to strengthen the defence industrial base, leveraging the defence Production Act Purchases and Industrial Base Analysis and Sustainment programs.The total budget request for these programs is US$1.5 billion. Meanwhile, US$163.4 million of the fiscal year 2025 budget request is allocated to hypersonic research and development efforts to address lead time and sub-tier 1 supplier issues for thermal protection and solid rocket motor technologies.

This priority for solid rocket motors extends from missile technology to space domain requirements. In fact, focusing on solid rocket motors is not new, but a continuation of a growing trend that contributes to increasing commercial activities. Just last year, the Army, Navy, and Air Force invested over US$100 million in new market entrants working to develop large solid rocket motors. In the past two years alone, a number of high-profile deals have taken place in the aerospace and defence industry: a US prime contractor acquired one of two solid rocket motor providers in the United States, and two prime contractors signed a strategic agreement to produce large quantities of rockets.

FUTURE SOLDIER TECHNOLOGIES AND INDUSTRY PERSPECTIVES

Geopolitical tensions contribute to much of the current and projected focus of defence spending. This impact is nowhere more evident than in the unmanned systems (aka drone) market. A year ago, some estimates valued the 2023 global military drone market as high as US$20.21 billion. Speed for unmanned systems will likely remain a focus in 2025. The fiscal year 2025 DoD budget request allocates a portion of the US$61.2 billion allocated for air power to unmanned aircraft systems such as the MQ-4 Triton and MQ-25 Stingray.

On the commercial front, operators are finding applications for unmanned aerial systems in various industries, including construction, real estate, infrastructure, oil and gas, agriculture, and logistics. In a groundbreaking decision for the US aviation industry, the Federal Aviation Administration will now allow simultaneous beyond-visual-line-of-sight flights for multiple commercial operators in the Dallas area. This, in addition to potential sanctions on foreign-made drones, could pave the way for further growth in unmanned aerial systems.



In the last decade, DoD budget requests for missile and munitions-related procurement and R&D have increased by 340%, from US$9 billion in fiscal year 2015 to US$30.6 billion in fiscal year 2024. These signs indicate that the industry can expect continued growth in the global solid rocket market through 2025.

The advanced air mobility (AAM) industry, largely focused on electric vertical takeoff and landing (eVTOL) aircraft, has seen interest and investment in recent years. Professional investors are increasingly interested in the potential of AAM, with 93% of the executive group responsible for over US$1.787 trillion in assets under management (AUM) showing interest in the eVTOL sector.eVTOL aircraft are quieter and more environmentally friendly compared to their counterparts thanks to their electric propulsion systems, and they cause zero operational emissions. While these systems are being considered for cargo transportation and military applications, the greatest value proposition is likely in the urban air mobility passenger market.

FUTURE SOLDIER TECHNOLOGIES AND INDUSTRY PERSPECTIVES

The year 2025 for the aerospace and defence industry can be defined by the word "operationalization". The industry is undergoing a continuous transformation, driven by advances in digital technologies, strategic investments, and a renewed focus on workforce development and supply chain visibility. From talent to supply chain opportunities, aerospace and defence companies are working to integrate digital technologies and artificial intelligence to address some of the industry's persistent challenges.

In after-sales services, AI applications for predictive maintenance have become well-known, but leading aerospace and defence companies will likely incorporate AI solutions into a more holistic approach to MRO evaluations. Similarly, we expect industry leaders to enhance their digital applications for supply chain visibility to address issues ranging from parts and labor shortages to concerns about parts quality and reliability. In the workforce, the strain is real, and pioneers are expected to give talent the same attention as production. In the area of new products, the industry is likely to see a few key players differentiating themselves through the operational flight of advanced air mobility and unmanned systems in commercial settings.Growth across the sector is likely to continue with technology underpinning every step. The myriad technologies implemented across the industry offer numerous opportunities for companies; these opportunities can help drive both margins and future innovation and capture the opportunities ahead.

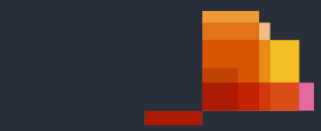
FUTURE SOLDIER TECHNOLOGIES AND INDUSTRY PERSPECTIVES

Here are the main trends that PwC sees for the aerospace and defence industry in 2025 and the next three years:

Portfolio reshaping: Demand for emerging technology and increased competition from new entrants have prompted major players to rethink their strategies. They are considering divesting non-core assets to simplify operations, consolidating capital to modernize core competencies, and sustaining innovation by acquiring venture capital-backed startups.

Geopolitical pressures: Increased defence budgets in Europe, Australia, and South Korea have significantly impacted sector growth. European countries, especially NATO members, have increased their spending due to the conflict in Ukraine. Australia has increased its defence investments in line with Indo-Pacific security priorities and initiatives such as AUKUS, a trilateral security partnership between Australia, the United Kingdom, and the United States. Similarly, South Korea has increased its defence budget against regional threats, focusing on missile defence and advanced technology. In the US, the new administration is expected to continue increasing defence spending with a domestic focus.

Partnerships and joint ventures (JVs): The sector increasingly prefers JVs over traditional acquisitions. This shift is due to JVs being less complex, having fewer regulatory hurdles, and providing greater protection against risks. JVs also support the development of enhanced capabilities through innovation obtained via collaboration.



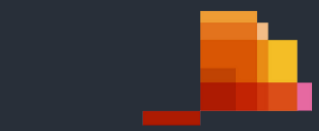
pwc

FUTURE SOLDIER TECHNOLOGIES AND INDUSTRY PERSPECTIVES

Strategic expansion in the space sector: : Mergers and acquisitions in the space sector have increased, driven by growing demand for satellite-based communication, defence capabilities, and low Earth orbit (LEO) infrastructure. Companies are increasingly acquiring others to build end-to-end capabilities in autonomous satellite networks and in-orbit services, in line with national security and commercial priorities. Additionally, the private sector's influence on new governance may elevate space as a strategic asset, encouraging further investment and innovation, and leading to greater consolidation of the sector.

Commercial consolidation: : Intensifying competition and operational inefficiencies are driving small and medium-sized aerospace companies towards strategic consolidation. Larger players are leveraging M&A to secure critical supply chain capabilities, particularly in high-demand segments like narrow-body aircraft and aftermarket services, reduce production bottlenecks, and achieve economies of scale.

We are seeing a significant trend toward increasing connectivity in supply chains—both within companies and beyond company walls. The result is a wealth of data that is now continuously accessible throughout the supply chain. Consequently, this is leading to supply chain ecosystems where partners can access relevant information in near real-time and simultaneously—so that decisions can be optimized and informed based on what is actually happening.



pwc

FUTURE SOLDIER TECHNOLOGIES AND INDUSTRY PERSPECTIVES

Alliedmarketresearch, which published a study on military robots and autonomous systems, shares the prediction that interest in artificial intelligence-based robots will increase in regions and countries where there are chemical, biological, radiological, and nuclear (CBRN) attack risks by 2030. The research, which emphasizes that companies that can provide reliability, hardware and software performance, and maintenance services in unmanned autonomous systems can be permanent, emphasizes that the need for unmanned ground vehicles will increase due to rescue and logistics needs. The study shares information that many countries have allocated budgets for unmanned helicopters and autonomous armed ground systems by 2030, while predicting that more than 30 projects are being tested in this area in America alone. In addition, unmanned ground vehicles in the tank category are expected to show rapid growth in the 5-year period.

IMARC, a research company that reports on sectoral transformations in technology, has also published its forecast that strong market growth will increase with the increase in operational efficiencies in military areas and the integration of systems with cybersecurity solutions. Sharing the prediction that a new market will emerge in the areas of disaster response, law enforcement, and search and rescue operations, IMARC included data that the use of bionic carrier robots or unmanned vehicles suitable for various terrain types, especially in tunnel, cave, and residential areas, will grow rapidly in a few years. According to the company, the market will exceed $31.8 billion by 2032 with the combination of human-machine collaboration and artificial intelligence.

Futuremarketresearch predicts that the robotics and autonomous systems (RAS) market will reach $27.5 billion by 2030. The research group, which also predicts that tactical mechanical technology and artificial intelligence autonomy will change the players in the sector, estimates that the impact of unmanned aerial systems against armored vehicles such as tanks and ships will improve, and that unmanned ground systems will be prioritized in terms of personnel safety and tactics.

FUTURE SOLDIER TECHNOLOGIES AND INDUSTRY PERSPECTIVES

Statzon, a research company, estimates the global military robot market to be $42.6 billion by 2030, noting that artificial intelligence, automation, and systems that perform high-risk tasks by reducing human casualties on the battlefield will show steady growth. The research, which states that advances in artificial intelligence and big data will increase the efficiency and autonomy of military robots, making them more capable in combat scenarios, notes that their capabilities, especially in tasks such as bomb disposal, casualty evacuation, and front-line surveillance, will be important in competition.

According to company forecasts, the most important markets will be North America, the Middle East and Africa, Europe, Asia Pacific, and South America, respectively. Company reports emphasize that the increasing dependence on digital infrastructure and the growing threats in the cyber domain will also increase the importance of telecommunications-related manufacturers, including communication and satellite technologies. They state that governments worldwide are investing more in advanced cyber defence capabilities, including secure networks, robust encryption systems, threat intelligence, and cyber response mechanisms, 1 and that artificial intelligence and the Internet of Things (IoT) investments will grow in the medium term, and that the cyber segment will show rapid growth due to the need for robust cyber defences. The military satellite market size, which is approximately $27 billion in 2024, is expected to exceed $40 billion by 2029.

Fortune Business Insights predicts this figure to be over $30 billion in the LEO, MEO, and GEO fields, and also shares in its forecasts the comment that rapid changes in technology and new players that may emerge in cube satellites could accelerate growth. Fortune Business Insights, which states that artificial intelligence applications to be used in the analysis of images obtained from satellites and the integration of these applications into military autonomous systems are also creating a new sector, predicts that the largest growth in military communication will be in small satellites with C3ISR capabilities.

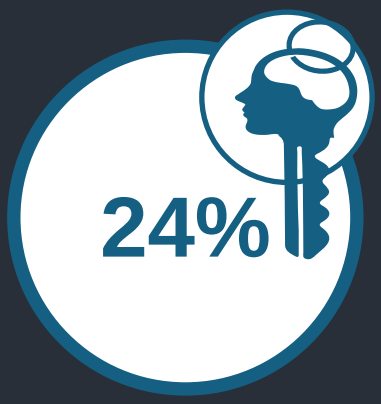
FUTURE SOLDIER TECHNOLOGIES AND INDUSTRY PERSPECTIVES

Global Market Insight reports that the global military satellite market was valued at $30.3 billion in 2024, while providing a large projection that the market, along with the small satellite market, could reach $73.3 billion in 2032. Satellites weighing over 1000 kilograms dominated the global market in 2023 with a revenue of $19 billion, while the largest players in the market are Raytheon, Northrop Grumman, and Airbus. The demand for products and solutions related to artificial intelligence, machine learning, and big data analytics to optimize defence operations, streamline logistics, improve information sharing, and ensure interoperability will increase rapidly in 5 years. Especially the rapid technological advancements and investments in defence platforms, systems, and technologies between China and America will be the most important factors in the rapid growth of the market.

Marketandmarkets and Futuremarketresearch predict that despite the risk of explosions and theft, there is also a high demand for ammunition stock, and that the market value of smart ammunition technologies will reach $33-35 billion by 2028. There is also data indicating that the largest and fastest growth in growth will be in the aviation sector.

Research companies report that the $2.5 trillion budget forecast for the defence industry in 2028 was realized in 2024, and that the spending growth between 2023 and 2024 was 4.9 percent. According to the companies, predictions that annual growth could be between 3-7 percent, especially based on developments in artificial intelligence, satellite and space technologies, and geopolitical developments, are not exaggerated.

TECHNOLOGY DEVELOPMENT PREDICTIONS BETWEEN 2025 & 2035



ARTIFICIAL INTELLIGENCE

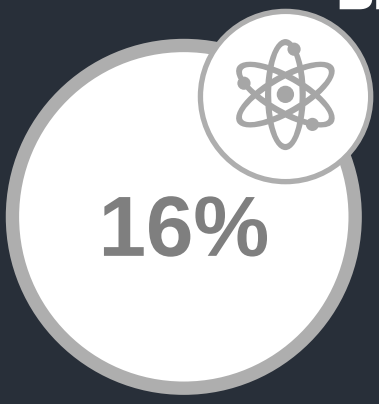
Computational reasoning for Intelligence,

Surveillance, Reconnaissance Leveraging digital twins and machine learning, and near-realistic testing in virtual environments

Decision-making engine for situational awareness

Using machine learning and data to deter threats and ensure mission success

Autonomous mission and cyber threat resilience



ADVANCED DEFENCE EQUIPMENT

Hypersonic flying systems

Directed energy weapons

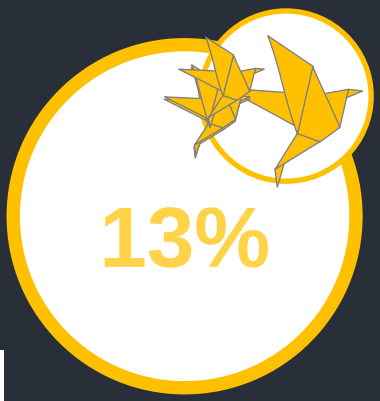
Weaponization of space

Electric propulsion and hydrogen fuel electrification techniques

Biotechnology and nanotechnology

Biometric sensors

Wearable technology



ROBOTICS AUTONOMOUS SYSTEMS

Force protection, enhancing situational awareness

Reducing soldier workload and challenging terrain solutions

Unmanned aerial, land, sea vehicles

Rock and sea mine clearance and explosive ordnance disposal,search, rescue, and robotic exoskeletons

Swarm and network algorithms

IOT

9%

MILITARY INTERNET OF THINGS

Connecting ships, aircraft, tanks, unmanned aerial vehicles, soldiers, and operation bases to a consistent and secure network

Integration of systems powered by informatics, artificial intelligence, and 5G&6G Technologies

Enhancing insights with biometric data and environmental monitoring

9%

CYBER WARFARE AND ELECTRONIC WARFARE

Addressing vulnerability concerns against cyber attacks and neutralizing rival systems,

Information loss prevention and technologies to damage systems

Artificial intelligence deception operations

Cyber threats against CBRN centers

Maintaining defence and response capabilities together

9%

IMMERSIVE TECHNOLOGIES

Creating repeatable and flexible experience environments

Enabling seamless collaboration with training and mission rehearsals in near-realistic virtual environments

Preparing personnel for missions with all technologies such as AR, VR, XR, MR

Virtual environments that enable testing the success, durability, energy, force, impact, and MRO factors of developed and manufactured systems in near-real conditions

6%

5G & 6G AND SPACE

Hyper compound connectivity and secure data infrastructure with 5G&6GDense, resilient battlefield infrastructure that enables the transfer of large amounts of data to remote sensors and weapons

Remote control and uninterrupted connectivity infrastructure for the entire infrastructure of unmanned systems

WiGL (Air-based network-based wireless charging and IoMT energy support, energy generation with wireless transmitters)

Technical infrastructure to ensure timely and appropriate information flow in military operations

Space-controlled and near-orbit dominance, microwave, anti-satellite missile and technology, kinetic energy, nuclear missile technologies

5%

BLOCKCHAIN BIG DATA AND ANALYTICS

Information infrastructure to be used in the analysis and simulation of information, which will become more concentrated with the use of technology

Effective interpretation of incoming data

Quantum technologies for analytical, fast, and secure data flow

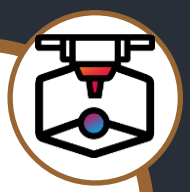
Quantum encryption, computing, cryptographic analysis, and sensor-based covert detection

Quantum mechanics and quantum-based powerful electronic system products

Analytical studies on the maneuver, destruction, and detection of unmanned vehicles

Blockchain infrastructure for the protection of classified military information and cyber threat prevention

Blockchain projects combining data analytics and artificial intelligence



5%

ADDITIVE MANUFACTURING

Durable productions that reduce weight, such as improving performance in speed, capacity, and fuel consumption

New design engineering products such as 3D printing technologies

Products that provide new combinations for armor, self-heating clothing, and ammunition

Initiatives for temporary part production, repair, material processing, and on-site assembly

Mobile micro-part productionMicrowave and thermal systems

Solutions providing lightweight or on-site manufacturing to ensure the long-term durability of robotic and autonomous systems

Speed-enhancing and on-site solution-producing, easily portable repair and supply methods

Products with low heat and delayed detection

Projects that will facilitate operational logistics processes and increase energy efficiency

Energy and logistics processes that reduce risk and minimize limitations in increasing operational complexities

4%

ENERGY AND LOGISTICS

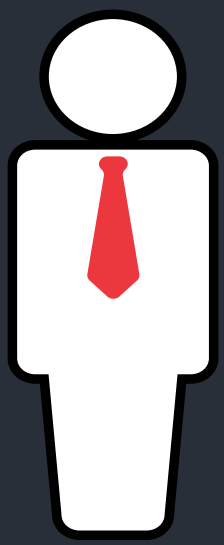
The data is from a study conducted by Startus Insight, a SaaS-based artificial intelligence-powered research platform that analyzes over 4.7 million startups worldwide.

Startus Insight analyzed 1,036 publicly tested projects in the field of new military technologies, examining which areas they were in and which areas were supported long-term, and then reviewed the top 10 defence and information sector projects.

Studies show that efforts are concentrated in Israel, the United Kingdom, and America, with increasing activity also observed in India, Germany, France, and the United Arab Emirates. Start-up projects such as Anduril, GeoSite, Epirus, Hermeus, Rebellion, Raven, Delfex, Geofabrika, and Taekion are also included in the evaluation.

It is commented that product development in the above-mentioned areas will accelerate between 2025-2030, and that studies in these technologies will shape the defence industry competition for the next 20 years.

The research highlights that Air defence Systems have shown a growth of 6.56% globally, emphasizing that this growth underscores the increasing global emphasis on air threats and the need for sophisticated systems to detect, track, and neutralize incoming threats. It is also acknowledged that countries' prioritization of airspace security, missile defence, and radar systems reflects this development in the sector.
Proactive Cybersecurity indicates another critical trend, supported by the addition of more than 2,600 new employees last year, with 320 companies and over 26,000 employees. This reflects an annual growth rate of 4.17%. This trend highlights the shifting focus towards preventive measures in cybersecurity.



ARTIFICIAL INTELLIGENCE RECOMMENDATIONS

Turkiye is at a globally competitive point, especially in areas such as autonomous weapon systems and unmanned aerial vehicles. However, more investment and long-term strategies are needed in areas such as quantum technologies and blockchain. Turkiye's strengths and rapidly growing defence industry can enable it to achieve a more advanced position in the future.

To strengthen its position, Turkiye will see the long-term effects of these advantages through technology transfer, facilitating and encouraging measures for the development of local ecosystems, and national strategies. At this point, measures can be taken in the following areas:

R&D investments can be increased, knowledge and experience accumulation can be accelerated by increasing agreements for technology transfer, and access to technology can be provided through agreements.

University-industry collaborations can be increased, academics and students can be included in projects. Academic research can be incorporated into start-up projects, and areas can be created for the industrialization of knowledge. Undergraduate and graduate programs should be developed in areas such as quantum, physics, artificial intelligence, cybersecurity, and blockchain.

Steps such as increasing the skilled human resources, national and collaborative efforts, regional alliances, cooperation with international R&D funds, and establishing a national ecosystem can accelerate the processes. It is possible to activate the existing infrastructure with a strong vision and coordination.

ARTIFICIAL INTELLIGENCE RECOMMENDATIONS

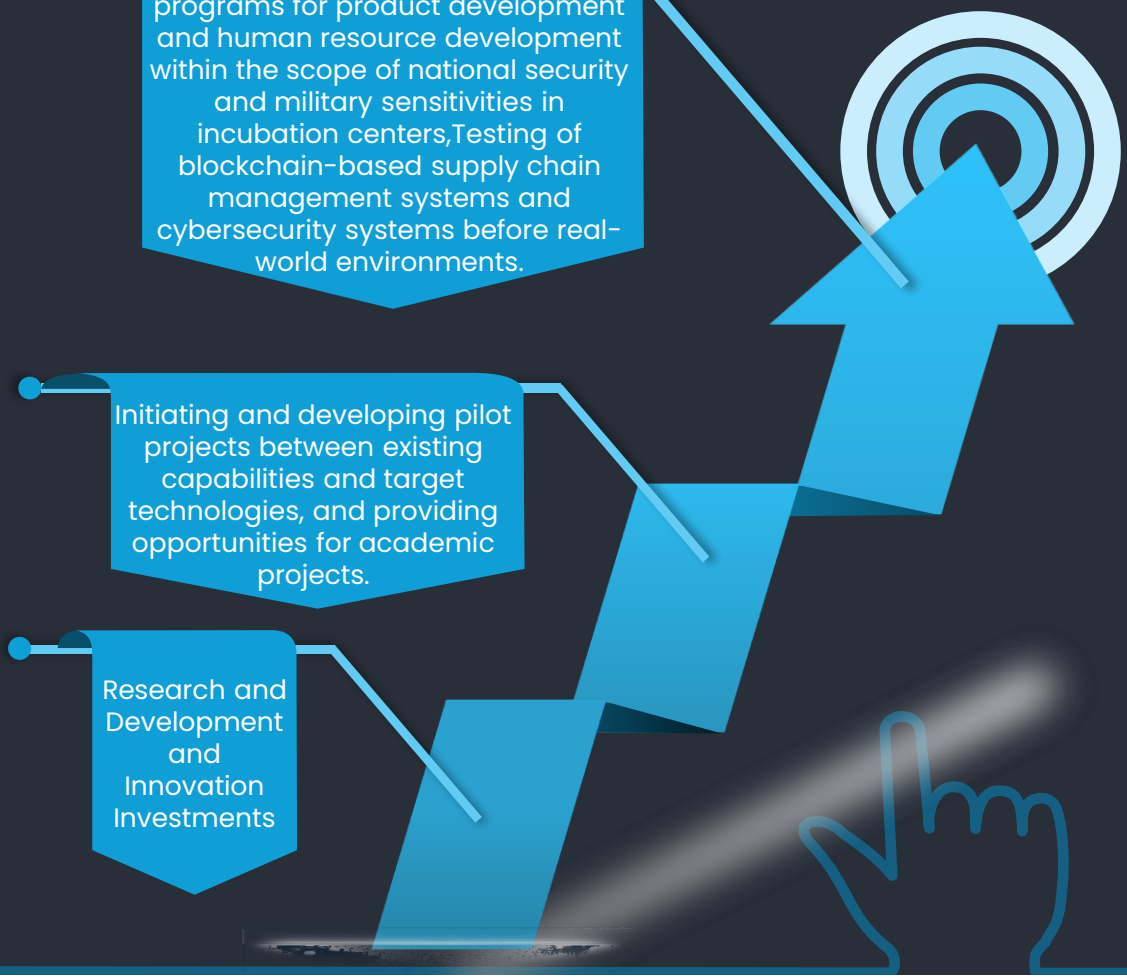
"Turkiye is at a globally competitive point, especially in areas such as autonomous weapon systems and unmanned aerial vehicles. However, more investment and long-term strategies are needed in areas such as quantum technologies and blockchain. Turkiye's strengths and rapidly growing defence industry can enable it to achieve a more advanced position in the future."

Target:
To strengthen the technological infrastructure and enhance core capabilities.

Implementation of national programs for product development and human resource development within the scope of national security and military sensitivities in incubation centers,Testing of blockchain-based supply chain management systems and cybersecurity systems before real-world environments.

Initiating and developing pilot projects between existing capabilities and target technologies, and providing opportunities for academic projects.

Research and Development and Innovation Investments



CONCLUSION

In the two-day organization, it was emphasized that production, investment and modernization approaches should be addressed with projections of a 5-10 year near future, 10-25 year medium term and 25-50 year long sustainable life cycle. The importance of cooperation between the private sector and public institutions in the production of sensitive and critical equipment was emphasized, and it was stated that the coordination in transforming academic studies into products should be done with a 'National mobilization' approach.

It is predicted that artificial intelligence will primarily be used in areas such as intelligence analysis, decision support tools, development of war tactics, simulation, and target detection, and it is thought that all countries are conducting artificial intelligence studies, particularly in autonomous swarms and electronic warfare. It is expected that artificial intelligence will increase its impact in the near future in terms of creating, organizing, and completing war strategies.

It is emphasized that satellite and telecommunication systems will be indispensable in future war environments and electronic warfare, and that, in this dimension, their critical importance as both a target and an advantage will increase. It has been pointed out that the importance of domestic products in environments where autonomous and robotic systems, smart munitions and hypersonic missiles, and 5th and 6th generation warplanes, such as air, land, sea, cyber and space technologies, will work together will increase even more. While the data that all these combined systems will receive from a large number of different platforms is prioritized as the most sensitive issue, the importance of data processing and the critical hosting, analysis and security measures for this data management have come to the fore as critical issues. In the communication and data evaluation stages, cyber security sensitivity has come to the fore in topics such as 'artificial intelligence', 'big data', 'internet of things', 'autonomous and robotic systems', and 'electronic warfare', and the importance of investments in this area has been expressed as a common concern.

It is predicted that the process that started with deepfake, with its digital twin and fake signal generation dimensions, will also be an important war multiplier for cyber attacks by generating fake data for artificial intelligence. Concerns have been shared that command and control systems will be the primary target in electronic warfare and cyber attacks in future wars.

Cyber attacks that halt, reduce, or misdirect the use of military hardware pose a risk of modern military forces being unable to fulfill their duties, even temporarily, and carry the potential to cause casualties and physical damage. Radio frequency-centered electronic warfare and the cyber domain are seen as an integrated area within the combined arms approach to gain information superiority and neutralize command-control networks. At this point, it has been recommended to carefully follow and develop blockchain and quantum technologies for the establishment of secure, fast communication networks in both data processing and protection, and electronic and cyber warfare domains. It has been noted that these technologies will be fundamental systems in secure data infrastructure and big data analysis, and that investments in this area will also be significant. Quantum sensing and computing, space-based sensors, and redundant communication networks are also highlighted as important areas for the military technological systems of the future.

It has been reminded that reducing foreign dependency in the domestic production of chip and sensor technologies, which are the basis of the systems used in the defence industry, is important in terms of national interests in eliminating the risks that may arise in extraordinary situations.

In the trend of Future Soldier technologies, it is assessed that in addition to robust, different and innovative product-oriented production in information technology-centered studies where hardware, software and cyber security areas come to the fore, productization that provides longer-range, faster, better communication that is compatible with mobility and provides technical support is also important in global competition.

While the applications and combinations of new technologies are seen as important as the technologies themselves, communication, methods of managing operations, the rate of damage and impact they will create, their autonomy and sustainability are also seen as the basic components of new generation technology in future military technologies.

The most fundamental concerns for future war environments are the reliability of machinery and technical infrastructure for remote warfare, while technologies that facilitate real-time detection and tracking, accelerate information flow, deter, prevent, or deceive, capabilities that increase maneuverability and resilience, a combination of cheaper sensors and big data analytics, and products that provide long-range, advanced destruction potential, and pinpoint accuracy will form the competitive areas in the defence field.

Laser, microwave and directed energy weapons, hypersonic weapon systems, energy production, storage and supply solutions, weapons of mass destruction, swarm air, land and sea systems and countermeasures, machine learning algorithms, durable-light efficient-innovative material and production techniques, microelectronics, next generation wireless technologies (FutureG), robot technologies, solutions for rapid assault and area defence are considered among the important dynamics of technology-centered warfare.

Measures for TEK-ER body protection, technologies to prevent infrared rays and detection, exoskeleton systems to support load carrying and mobility, mobile energy production for electronic systems to be used, continuity of intelligence and communication, armors developed against drones, physical and psychological adaptation training of field and desk personnel to technological developments, the realism of simulation training and training methods with different scenarios, and the need for personnel with intelligence and analytical skills have also come to the fore as the most important issues.

It has been noted that the 'logistics support analysis' process should begin with the design phase for the long-lasting and efficient use of products, otherwise, products may bring serious costs or create operational risks, and this issue should be considered as a critical issue.

Until systems, concepts, and capabilities are tested in a prolonged conflict against a real enemy, predictions about future wars can be made. We believe that the evaluations of this 'Future Soldier 2024' organization will be a guide for defence industry stakeholders on the path from idea to design, from production to marketing and branding.

Best Regards

SASAD