RUSSIAN-UKRAINIAN TECHNOLOGICAL WAR

THORNIKE ZEDELASHVILI
Doctor in PhD Political Science, employee of the Information Security Department of the Digital Governance Agency of the Ministry of Justice, founder of the online publication „Leader“, invited lecturer at the Caucasus International University.
E-Mail: thomaszedelashvili@gmail.com
ORCID: 0000-0003-2630-1779

Abstract: The Black Sea region is a priority region, where six countries are involved – Russia, Turkey, Ukraine, Romania, Bulgaria and Georgia. Of course, of these countries, Russia has the greatest influence on the Black Sea region, followed by Turkey. Accordingly, the Russian-Ukrainian war poses great political, economic and social risks both in the South Caucasus and in the entire Black Sea region. Especially when the world is in such a phase of technological achievements, when there is active talk of replacing soldiers with robots. To some extent, this is already working, experts call this war a technological war, and this also has a certain impact on its duration. The Black Sea states need new technological protection. The use of modern technologies has contributed significantly to the colossal losses of the Russian-Ukrainian war – many people have died and infrastructure has been destroyed. This conflict includes a large amount of cyberattacks, disinformation, economic pressure, and components of hybrid warfare. This is not new, Ukraine receives modern equipment from the United States, NATO, the European Union, Great Britain, Germany, France, Poland, and other European countries. The use of new technologies, such as cyber warfare, the use of artificial intelligence, can be said to already affect geopolitics and military operations with potential benefits, on the one hand, by reducing losses in the defensive direction, and on the other hand, by increasing losses in the event of an attack, providing detailed target information, and assisting in logistical issues. AI is also used in information and psychological warfare. Artificial intelligence technologies are actively used in cyberattacks, which creates a very dangerous reality.

Keywords: artificial intelligence; cyberattacks; cyberwar; Black Sea region; technologies; disinformation; hybrid war.

* * *

10 key technologies used in the Russian-Ukrainian war:

- ***Artillery and missile systems;***
- ***Artificial intelligence (AI);***
- ***Cyberattacks;***
- ***Social Media;***
- ***Drones;***
- ***Satellites;***
- ***Telecoms Sans Frontières (TSF);***
- ***Electronic warfare;***
- ***Consumer technology and applications;***
- ***VR and 3D holograms (VR & 3D holograms),***

including the latest technologies, platforms in the direction of artificial intelligence, which helps in making and implementing various decisions – „RZ-500 attack drone, reconnaissance drone PD-1 / PD-2, Hunter RSVK-M2 unmanned military vehicles, anti-aircraft missile system Stugna-P, ST-35 Silent Thunder mobile combat aircraft“ (Kryvenko P.)

Artillery missile systems

Russia has used various types of artillery and missile systems – rocket launchers, howitzers, ballistic missiles, etc. to bombard targets in Ukrainian-controlled territories. According to the Ukrainian Communications Service, as of October 2022, more than 4,000 base stations, 60,000 km. of fiber-optic lines and 18 broadcasting antennas have been destroyed, damaged or stolen.

The use of Javelin anti-tank munitions manufactured in the United States makes things easier for Ukrainians. Also helping is the software of the American technology company Palantir, it is now possible to easily target Russian tanks and artillery. It helps to visually display the positions of the army from commercial satellites and social media channels and then destroy them. Thermal imaging technology facilitates digital targeting capabilities. (AI)

Ukraine is using a large part of its AI technology for defense. Ukrainian AI company Primer has replaced its commercial AI voice transcription and translation services with AI to enable the country to process data from Russian communications networks.

The Russia-Ukraine conflict can be considered the first war in which advanced AI technologies have been used – for example, facial recognition software. It is known that *„in March 2022, the Ukrainian Defense Ministry launched a new image and facial recognition program developed by the American company Clearview AI, which is based on artificial intelligence and thereby determines the identities of fallen soldiers, as well as the identities of Russian attackers.“* (Fontes R.)

In the Russia-Ukraine war, an artificial intelligence-based tool called MetaConstellation is being used with the help of the company Palantir, this tool allows Ukraine and its allies to have access to commercial data. Practice has shown that commercial companies have a lot of useful information – for example, *„optical imagery, synthetic aperture radar imagery – this refers to aerial imagery; thermal imaging, which refers to the detection of artillery and missile fire. It is known that the sources of this data are various scientific institutions that conduct atmospheric research – for example: Airbus, Capella, Maxar and others.“* (re-russia.net)

The company „evaluated data collected by approximately 40 commercial satellites,“ (re-russia.net) This allowed the Ukrainian side to obtain relief images, which implies a focus of up to three square meters. Also, Ukrainian officers have the opportunity to use computer tablets to easily and in real time provide the information we talked about above. In this case, analysts name the only problem as the availability of high-quality Internet.

Alex Karp, CEO of Palantir, says that „the artificial intelligence technology used changes the competitive advantage of small countries against large ones.“ (Fontes R.)

Cyberattacks

Russia carried out its first cyberattacks before the war began, these were DDoS attacks. Russian hacking groups used the well-known „Trojan horse“ malware against the systems of Ukrainian government agencies, which Microsoft called „FoxBlade“ (which can be translated into Georgian as „Fox Blade“, meaning that the Russian attackers wanted to cut off the Internet connection and paralyze the Ukrainian command and control centers).

The Microsoft report notes that this was observed by ethical hackers from the United States, various groups. Ukraine was able to defend itself due to quick actions – technological structures quickly distributed digital infrastructure on public „cloud“ storage facilities, the data centers of which are located in various European countries. Microsoft says it has discovered an illegal intrusion attempt by Russian-hired hacking groups in 42 countries, involving the systems of 128 organizations. The hacktivist group Anonymous supported Ukraine in this war and responded with retaliatory cyberattacks against the Russian Federation, which led to disruptions in government systems, various TV channels, and video platforms. Anonymous obtained a list of Russian agents, part of which it has made public. However, much of it remains secret. The Ukrainian IT army, which is supported by the Ukrainian government, is

also involved in this cyberwar. In the first half of 2022, 22 percent of Ukraine's fiber optic network was damaged or destroyed, and 1,350 powerful cyberattacks were recorded. In the second half of 2022, 2,194 powerful cyberattacks were recorded, and the damage is still being calculated.

On February 16, 2022, the websites of almost all government structures were blocked. Russia openly demands: NATO should not expand towards Eastern Europe, Ukraine and Georgia cannot become members of this organization. Russia categorically demanded that the United States and Europe reconsider the decision made at the Brussels summit and withdraw the strategy of expansion towards Eastern Europe. Russia has great capabilities in terms of cyberwarfare and a number of events confirm this, but its capabilities also have limits. NATO published a communiqué, where it was written that the 2008 Bucharest decision remains in force. The communiqué emphasizes that „Georgia and Ukraine will definitely become members of the alliance.“ (საქართველოს საზოგადოებრივი მაუწყებელი) The decision taken at the Bucharest summit did not slow down Russia.

According to Cisco, *„The massive cyberattacks were carried out on February 15, 2022, and the second on February 24. Following this, CISA and the FBI issued joint cybersecurity recommendations on March 17, urging users of US and international satellite communication network providers (SATCOM) to be prepared for potential threats. This warning followed the cyberattacks on February 24, when attacks were carried out on Viasat and KA-SAT, which disrupted broadband satellite Internet in Ukraine and other European countries.“* (Cisco Annual Report) All states around the world should be on alert – various actors, who excel in hacking, fraud and infrastructure-damaging attacks, are trying to profit from – using the Russian-Ukrainian conflict as a kind of tool. For example, spreading news, disinformation, soliciting donations with malicious links, names and fake web addresses of aid funds or fake websites supporting refugees, etc.

The State Special Communications Service of Ukraine published a report on Russian cyberattacks and cyberstrategy during the war, which states emphatically:

"On November 24, Russia launched powerful cyberattacks on Ukraine's critical infrastructure, in particular energy facilities, in order to disrupt electricity supplies. In parallel with the cyberattacks, the Russian Federation also carried out targeted bombing.“ (cyberscoop.com)

As we have mentioned, various hacking groups are involved in these cyberattacks at different levels. When Russia invaded Ukraine and launched a conventional war, this was preceded by traditional cyberattacks, which continue to this day. There is a hacktivist group called Anonymous Sudan. According to experts, it is a Russian group of malicious hackers, which is directly connected to the Russian hacktivist group Killnet. This hacktivist group has stated that it supports the Russian Federation in the Russian-Ukrainian war, therefore it often acts against Ukraine. In March 2023, Anonymous Sudan and Killnet jointly claimed responsibility for many cyberattacks, including attacks on Latvian government agencies, NASA systems, and Ukrainian systems. Both individually and jointly, they carried out DDoS attacks on French hospitals, universities, airports, and the systems of the Ministries of Justice and the Interior. Killnet's targets included all countries that provide some form of assistance to Ukraine, except for the United States. The hacktivist group launched cyberattacks in February on more than a dozen hospitals in the United States *„(Stanford Health, Michigan Medicine, Duke Health, and Cedar-Sinai, among others).“* (research.checkpoint.com) In October, it carried out DDoS attacks on several airports in the United States *„(Los Angeles International Airport, Chicago O'Hare International Airport, Hartsfield-Jackson Atlanta International Airport, etc.)“,* (research.checkpoint.com) This led to the suspension and paralysis of flights.

Killnet completely shifted its focus to supporting Russia's geopolitical interests in April 2022. According to its statement, „more than 550 cyberattacks were carried out, of which 45 were attacks on Ukrainian systems, which is less than 10 percent of the total attacks.“ (research.checkpoint.com)

One of the *„targets was Elon Musk's broadband satellite network Starlink, which was subjected to cyberattacks, as a result of which on November 18 many users complained that they were unable to log*

in to their accounts for several hours. Various groups were also involved in carrying out these cyberattacks – for example, the hacking groups Radis, Halva, Anonymous Russian, and others.“ (Bracken B.) *Killnet launched a cyberattack on the White House website on November 17, calling it a „30-minute test attack.“* (Bracken B.) Rob Joyce, director of the U.S. National Cybersecurity Agency, said:

“They are targeting closed-circuit television cameras that local governments and private businesses use to monitor the environment. We are seeing Russian hackers accessing public webcams that are accessible to everyone. However, Russian hackers are also using this to monitor aid convoys and trains. We know that the Russians are also monitoring logistics companies to learn more about the delivery of weapons to Ukraine.“ (theguardian.com)

The war launched by Russia in Ukraine has shattered not only the myth of Russia's invincibility from a military perspective, but also from a cyberwar perspective. Immediately after the war began, hackers in Russia hacked video platforms Wink and IVI, and instead of TV series, several Russian channels broadcast videos about the bombings in Ukraine from „Nastoyashchee Vremya“ and „Dozhd“. Anonymous tweeted about the broadcast of war footage on Russian channels and also released a video. Anonymous, which is a free, decentralized hacker organization that unites so-called hacktivists, published a statement that they had penetrated Russian security systems and obtained lists of Russian agents, which they would gradually publish by state.

Cyber threat analysts have compiled a table of cyber groups involved in the Russia-Ukraine conflict, allowing us to conduct analysis to assess the cyber threat landscape. Russian-sponsored advanced threat groups (APTs) have demonstrated the ability to maintain persistent, undetected, long-term access and unauthorized access to networks using legitimate credentials. They pose the highest risk of cyber attacks, such as: „APT28, Turla, Gamaredon, Energetic Bear, APT29, Sandworm and others“.

Social media

The Russia-Ukraine war is a war where the Internet is used to the greatest extent, where a lot of information and disinformation is spread, in the form of text, photos and videos. Various social networks and social media platforms are actively used. There is a lot of activity on social networks and in the media – family members and friends are publishing posts, information, video and photo materials, contacting acquaintances, friends, and family members to inform them of their safety and location, that they are alive. It is known that many large technology companies have somewhat limited the propaganda and spread of disinformation by Russian media outlets. The visibility of posts on Facebook and Twitter has also been limited.

Drones

Russia and Ukraine have used far more unmanned aerial vehicles in the war than in any other war. Drones have proven to be highly effective for reconnaissance and surveillance. The Ukrainian military has also used drones to scout and target enemy positions using precision-guided munitions. It is known that the unmanned aerial vehicles most often used by the Ukrainian side are very simple, ordinary commercial drones, which have integrated high-resolution cameras that are connected to smartphones.

For example, the Turkish Bayraktar TB2 aircraft carries laser-guided bombs that target vehicles, military groups, and military bases. There are the American-made Switchblade and the Russian-made Lantset, these are the so-called „kamikaze drones.“ They can be carried by one person even in a backpack. They have warheads built into them, which means that they hit the target and explode.

Given the unprecedented increase in the use of drones in the Russia-Ukraine war, both sides have developed counter-drone systems to detect and eliminate enemy unmanned aerial vehicles. For example, the Ukrainian side uses anti-drone systems, such as the Turkish-made KARGU. It can monitor and destroy targets.

Satellites

As for satellites, after Russia's invasion of Ukraine, 5,000 Starlink broadband satellites have been providing Ukraine with internet access. This has been crucial to helping citizens and the government stay connected and better coordinate. To date, approximately 25,000 Starlink terminals are operational to support Ukraine's defense and connectivity (TSF).

This is the world's first non-governmental organization focused on emergency response technologies. The organization's goal is to build rapid response communication centers worldwide. TSF teams have been able to provide emergency telecommunications equipment to refugees both inside and outside Ukraine. It is known that more than eight million people have left Ukraine since the Russian invasion. They have sought asylum in various countries, and more than six million people have become internally displaced. This is 32 percent of the population of Ukraine.

Electronic warfare (EW)

A major issue in the Russo-Ukrainian war was the use of electronic warfare (EW) systems. This includes jamming communications, radar, and other electronic systems.

In February, before Russia began the war, employees of the technology company HawkEye 360, using commercial satellites, which include the Global Positioning System (GPS), detected a violation of the border along the Ukrainian-Belarusian border, north of Chernobyl, by unmanned aerial vehicles that crossed the border, moving in the Luhansk and Donetsk regions. The Ukrainian military used electronic warfare systems to block Russian communications and GPS signals, which ensured the protection of communications infrastructure.

Electronic warfare systems are any configuration of technologies designed and built on one or more air, land, sea, or space platforms to perform military or intelligence missions.

Consumer Technology and Applications

In 2020, the mobile application and online portal Diia was launched, which was a traditional government system used to issue licensing permits, purchase parking tickets, which was transformed after the war began so that civilians could upload photos with geolocation coordinates of various Russian military activities, or disseminate information about suspicious people.

For example, in March 2022, the secure chat system eVorog (eEnemy), which can be used on Telegram, began operating, allowing civilians to share a wealth of information about the activity and movement of troops. The chat system turned Ukrainian citizens with smartphones into digital resistance fighters – people gather in one space and conduct military reconnaissance.

Virtual Reality (VR) and 3D Holograms

The Ukrainian military has been using virtual reality (VR) training systems, which simulate combat scenarios to train soldiers on tactics and procedures. This type of training allowed soldiers to practice in a safe and controlled environment before they went directly to the front lines.

In June 2022, Volodymyr Zelenskyy used ARHT Media's 3D holographic technology to address more than 200,000 top tech entrepreneurs, investors, and corporate leaders at seven major technology events in Europe.

It is also important to highlight the problematic issues of using artificial intelligence components in conventional warfare. One of the problems with the use of artificial intelligence in military systems is its vulnerability to special attacks, that is, attacks that are directly directed against the hardware software – even a minor change in data input can lead to incorrect information processing results, which can be catastrophic in the process of combat. Humanity is striving for a world where new technologies will replace the old, standard war, changing the dynamics of war through technological accessibility.

Experts have already talked about the possibility that the Russian-Ukrainian war may be a kind of testing period for artificial intelligence and new technologies in general – in addition to what we have

listed, new technological inventions of artificial intelligence components will be tested. The use of new technological components does affect the process of conventional warfare, but it still cannot determine it as a whole. How can new technologies and the development of artificial intelligence components change the entire essence of war?

For example, we can cite the fact that occurred in 1988: „A US Navy cruiser named „Aegis" mistakenly shot down an Iranian passenger plane because the tactical operations officer in the combat information center misjudged the information, based on various data, he thought that it was a hostile Iranian military aircraft. As a result, about 300 civilians were killed." (Stavridis J.)

In this case, we can assume that if artificial intelligence systems had been available at that time, which could analyze a large amount of data, they would certainly have revealed that this was a civilian aircraft and people would have survived. Artificial intelligence can provide us with detailed and strategic information at various specific moments, which allows decision-makers to use precise weapons.

People who are familiar with high technological achievements are concerned about one of the most important issues – as they improve, weapons become smarter every day, and at the same time it becomes easier to kill. Accordingly, leading countries are working on developing regulations to establish norms. NATO, the European Union, the United States, Great Britain and other European countries are taking this issue seriously.

There are aggressor countries in the world (such as Russia) and there are hacker-terrorist groups that use technological achievements for evil purposes. Currently, technological advances are growing very rapidly, both in virtual and real space, including the use of artificial intelligence components, this is exacerbated by the geopolitical situation that has developed worldwide, and specifically on the Black Sea coast. This was actually caused by Russia's aggression against Ukraine. A lot of time has passed since February 24, 2022, and the Russian army continues to conduct ground, air operations and cyber-attacks throughout the territory of a sovereign state.

Conclusion

We do not know how long the war will last. It is true that advanced countries are intensively helping Ukraine, but according to analysts, this is not enough. What happens in the conditions of a real war, almost the same thing happens in the conditions of a virtual war, that is, in the Internet space. It is impossible to discuss these two events separately. Ukraine needs defense systems equipped with the latest technologies not only in the form of weapons, but also in terms of new technologies. Great attention, equipping, observation, study and action are needed.

Today, the Russian government often mentions nuclear weapons. We all know that this will be a complete catastrophe for humanity. It is not excluded that in this case we are dealing with propaganda launched only for the purpose of intimidation, but knowing the character and nature of Russia, we cannot trust the Kremlin, it is really capable of this. Therefore, the whole world is obliged to resist Russian aggression – NATO, the European Union, the United States of America must develop effective programs that will detail assistance to Ukraine. In fact, all leading countries must have their say and show it with action. Recently, they have even started talking about the fact that this war must definitely end and the issues be resolved at the round table. Naturally, all wars end at some point, but in this case there is a dilemma – Russia does not retreat, does not give up the conquered territories, the Ukrainian government does not give up, of course, does not recognize the occupied territories, so how should the war in the Black Sea region end? At this stage, we can assume that the current situation will be preserved and then the war will resume at any time, in any case, the situation will always be explosive. Probably, a lot will depend on how the elections in the United States of America will be held and who will come to power. However, whoever takes power, they will still not be able to warm up Russian-Ukrainian relations and return them to their original state, as I have already mentioned, the current situation may freeze and this may be called the end of the war. At this stage, there is no other given. It should also be noted that neither the EU nor the US administration officials are talking about ending the war, they are mobilizing to increase aid to Ukraine. Whether this is a good thing or a bad thing, the near future will show.

Bibliography:

Bracken B. *„Killnet Gloats About DDoS Attacks Downing Starlink“, darkreading.com.* 29 november 2022. 10 01 2025.

Cisco Annual Report. *Reimagining the future of connectivity*. Research. USA: Cisco, 2022.

cyberscoop.com. *„Ukraine warns of ‘massive cyberattacks’ coming from Russia on critical infrastructure sites“*. 26 08 2022. 10 01 2025.

Fontes R., Kamminga J.,. *„Ukraine A Living Lab for AI Warfare“, nationaldefensemagazine.org,*. 24 03 2023. 10 01 2025.

Kryvenko P. *„Artificial Intelligence in the Russian-Ukrainian war“, newgeopolitics.org.* 13 june 2022. 10 january 2025.

re-russia.net. *„A natural ally: Artificial intelligence is becoming an increasingly important tool in warfare, but it requires access to an extensive civilian digital infrastructure“*. 14 04 2023. 10 01 2025.

research.checkpoint.com. *„The New Era of Hacktivism – State-Mobilized Hacktivism Proliferates to the West and Beyond“*. 29 08 2022. 10 01 2025.

Stavridis J. *„The Russia-Ukraine war may become a testing ground for AI“, livemint.com.* 01 jun 2023. 10 01 2025.

theguardian.com. *„Russian hackers ‘target security cameras inside Ukraine coffee shops“*. 11 04 2023. 10 01 2025.

theguardian.com, Russian hackers ‘target security cameras inside Ukraine coffee shops“. n.d.

საქართველოს საზოგადოებრივი მაუწყებელი. *„ბრიუსელის სამიტი და ნატოს კომუნიკე“, 1tv.ge,*. 14 06 2021. 10 01 2025.