ACADEMY OF ARMED FORCES
MILITARY SCIENTIFIC RESEARCH INSTITUTE
THEORETICAL-SCIENTIFIC JOURNAL
DECEMBER 2024

MILITARY JOURNAL

(Fourth edition)

Publication of Academy of Armed Forces
Approved by decision no. 4, dated 25.11.2024
of the Military Journal Managing Board

Prepared for publication by:

Editing and Publishing Group
Military Scientific Research Institute (MSRI)

Translated in english by the Translation/Teaching Group in the Department of Foreign Languages:

Shpëtim Madani	Kejdi Budo (Sheri)
Erin Dini	Daniela Dyrmishi
Greta Përgjegji	Esmeralda Bërdo
Çetina Hyka	Alba Hysi
Bledar Vrapi	Ilda Basha
Klodiana Tavanxhiu	Anda Zilja
Manjola Likaj	Eva Reveli
Alma Vladi	Monika Myrto

ISSN 2227-8133 (Print), ISSN 2227-8141 (Online)

Copies: 150

Dear readers!

The fourth edition of the "Military Journal", December 2024, is a reprint of selected articles of the three MJ editions, translated into English.

Armed Forces Academy
Military Scientific Research Institute
Printed: December 2024

TABLE OF CONTENTS

FIRST RUBRIC

SECURITY AND DEFENSE ANALYSIS AND ASSESSMENTS

Technological revolution, "proxy wars[1]", "army of none[2]" and "false flag operations[3]", challenges and opportunities for future military operations

Colonel Msc. Ulsi REXHAJ
Director of the Military Scientific Research Institute
Colonel Msc. Hysni GJERGJI
Head of Department at the Military Scientific Research Institute

Abstract

The current war environment turns out to be a mix of global economic, political, military and technological instability on a scale never seen before.[4] Keyboard-and-mouse warfare is a new form of conflict, where states or international organizations engage in actions aimed at targeting, challenging, or disrupting another state's technological and military infrastructure.

Over the last decade, numerous NATO and non-NATO[5] states have recognized and accepted cyberspace as the 5th domain of warfare, alongside land, sea, air and outer space. At the Washington summit that is expected to be held on July 9 to 11 of this year[6], a primary focus of discussions will be the technological revolutionization of the Alliance, particularly in the light of the era of artificial intelligence of warfare. The Armed Forces, being the main instrument in the national power of a nation[7], have

[1] https://dictionary.cambridge.org/dictionary/english/proxy-war

[2] https://www.shtepiaelibrit.com/store/sq/historia-aktualityte/7520--ushtria-e-askujt-paul-scharre-9789928286987.html

[3] https://dictionary.cambridge.org/dictionary/english/false-flag

[4] Major General Robert H. Latiff, Commander of the US Air Force, in "Future war preparation" (2017).

[5] https://www.ncia.nato.int/about-us/newsroom/save-the-date-nato-edge-2024.html

[6] https://www.nato.int/cps/en/natohq/topics_50115.htm

[7] DIME – Instruments of national power: Diplomacy, Intelligence, Military Forces, Economy

have become a key target for opposing states or organizations. Thus, Albania, as part of the largest political-military Alliance, has also been a target of attacks by these actors for this reason as well[8]*. This paper will analyze the expansion of digitalization within the military field, which has promoted development on the one hand, but has also raised serious concerns related to the security of this invisible, intangible and borderless configured space. Emerging new wars, such as those in Ukraine, Gaza or elsewhere, often conceal underlying economic, political, and military benefits or interests, or all three of them, taking shape as proxy wars, involving mercenaries and other deniable means.*[9]

Keywords: NATO, *proxy* war, armed force, cyber warfare domain, army of none, false flag operation.

1. The technological evolution of war, towards the cyber domain and artificial intelligence

In 2024, the world is more advanced, with information technology enhancing relations among people and states, including the way in which war in general and armed conflicts in particular are conducted and managed. Since the first conflicts of social groups, organized in tribes or empires, have started mainly with the aim of expanding territories rich in essential resources such as minerals, plants, animals., etc. The capture of more land surface by one side and the protection of these spaces by the other side has accompanied humanity for many centuries.[10] With the invention of warships and fleets, the warfare moved to another space, the maritime one, where the actors aimed for as much access to the oceans as possible for both the resources they provided and the passageways they offered. The airplane and human flight capabilities led to military powers equipped with air fleets gaining superiority in the air, which in turn provided superiority on land and sea as well. Today, human society has entered the stage of daily use and interdependence of the Internet. Currently, we are dependent on cyberspace for everything from commerce to communication, significantly reshaping our lifestyles, our habits, but even the concept of armed conflict. The wars until today have been fought in a certain geographical region and in a certain period of time. Today, the nature of warfare has changed completely with the recognition of its cyber component. Physical borders no longer exist, the warfront has lost its meaning, and the warring actors no longer need to face each other in person and have direct contact.

NATO has recognized "cyberspace" as a domain for the development of NATO's combat operations, acknowledging the need of the alliance to exercise and train to defend itself and its members, as well as in other areas of development of warfare

[8] https://www.zeriamerices.com/a/6734669.html

[9] https://shp.al/sq/a-ka-nje-shkak-lufta-ne-ukraine/

[10] The ongoing wars of Israel with Palestine and Russia against Ukraine prove this thesis.

(sea, land, air, space). The cyber threats are now so significant that a small number of hackers can bring a nation to its knees in minutes, by targeting critical state and military infrastructure, power plants, transportation networks, ports, airports, hospitals and government offices. One of the first cases of such an attack was recorded in 2007, when a massive wave of Russian cyberattacks targeted Estonia over three weeks, causing the complete paralysis of Estonian ministries, banks and communication companies. In 2013, Ukraine experienced a similar large-scale cyber assault, resulting in a total power outage and widespread paralysis, also attributed to Russian cyber operations. These were the first attacks that also served as the first warning of cyber attacks for NATO, which had begun to expand into former Soviet republics. The trend of cyber incidents in 2022-2023 is considered alarming, with a notable increase and a shift from attacks against civilian targets to government targets and infrastructure. From Albania's point of view as a NATO member, the cyberattacks, based on the methods they use and selected targets, are primarily acts of sabotage aimed at disrupting vital economic, military, and strategic points in our country, and therefore also of NATO. Another threat arises from attacks on sensitive national information systems, where data is stolen, manipulated, or destroyed. This espionage activity is mainly directed by intelligence services hostile to NATO, targeting one or more member states of the Alliance, since the modernization of technology has also transformed the way of doing espionage. In the digital age, there is no need to physically break into safes to access a country's military plans, resources, or strategies. Instead, a skilled hacker can remotely retrieve and exploit sensitive documents without any physical contact, often leaving little to no trace of their actions.

The criminal and hostile activity that NATO's opposing state actors can undertake against the members of the alliance can also be classified as subversive actions, since is one of the consequences of a cyberattacks is undermining and losing public trust in security institutions. When cyberattacks hit civilian targets in order to achieve their political objectives by spreading fear, uncertainty and terror, then such attacks meet the conditions of being defined as terrorist actions. Armed conflict in cyber space on the one hand requires cyber security, but on the other hand this security is not only a technical subject, as is often said, but it is a strategy, policy, doctrine, action procedure, and even a war instrument. Based on the analyzed cases and the trends in technological development, there is a growing awareness among the law enforcement structures to adapt necessary countermeasures to face this new multi-dimensional threat. "A cyberattack targeting one or more members of the Alliance, given its potential consequences equivalent to those of a military attack, also providing for the response of NATO's armed structures against this threat of the century[11]". There has been a definitive shift away from American unipolarity, with China and Russia benefiting from this retreat. The geopolitical axis of power is clearly realigning with

[11] Statement by NATO Secretary General Jens Stoltenberg during the meeting with the Alliance´s defense ministers on June 28, 2017.

the US and the EU on one side and an anti-US axis compromising China, Iran, Russia and North Korea on the other. This realignment is leading to bolder, less predictable actions and a more dangerous and uncertain global environment. We will continue to witness this change in 2024, which may be worsened by the stance of non-aligned countries and the rise of competitive blocs such as BRICS (Brazil, Russia, India, China).

Even if we are not directly engaged in wars, it is crucial to study them, learn from both the mistakes and the advantages, even if those advantages belong to the opponent. We do not need to refer to history as firstly, this threat is new and secondly the Russian aggression against Ukraine along with the attack of Hamas on Israel mark the massive and challenging use of technology in military conflicts. The current warfare environment turns out to be a blend of global economic, political, military and technological instability on a scale never seen before.[12]" Almost any means can be considered an act of war, with the critical line often drawn at the control and domination of one group, over a group or over other people.[13] Hamas' attack on October 7 marked a failure in monitoring key electronic communication channels used by Palestinian attackers. Falling into the trap of Hamas operatives who knew they were being overheard, communicating covertly with each other with messages denying an attack on Israel[14]. The over-reliance on border surveillance technology devices that were easily disabled by attackers, allowed terrorists to launch raid on military bases, killing soldiers while they slept[15], making it a painful lesson for the Israelis.

The operational failure was the concentration of leaders from the Gaza division in a single location along the border. When the base was overrun, most of the senior officers were killed, wounded or taken hostage. This concentration of commanders at a single border base that was hit in the first phase of the attack also prevented communication with the rest of the armed forces. The Israeli military was confident in the impenetrability of the technological system they possessed. Israeli soldiers blindly trusted the technology and were not able to watch the videos manipulated by Hamas[16]. The wall and technological means of encircling Gaza proved to be easier to overcome, making the human factor indispensable in the conduct of cyberwar. The simultaneous combination of the use of "Wagner" in Ukraine, "Hamas" in the Persian Gulf and "Houthi" in the Red Sea, has introduced the world into a new stage and form of war.

Based on the established trend, there is no doubt that the definition of "war" will evolve, potentially leading a new definition of what will be called a combatant and

[12] Major General Robert H. Latiff Commander of the US Air Force, "Future war preparatin" (2017).
[13] Naz Modirzadeh, Harvard Law School Program on International Law and Armed Conflict (PILAC).
[14] Tzachi Hanegbi, Israel's national security adviser, in a radio interview six days prior to the attack.
[15] Statement of Brig. Gen. Dan Goldfuss, the Israeli commander who helped lead the counterattack.
[16] https://www.nytimes.com/by/patrick-kingsley

a warring party. Individuals, who, although hiding in many ways and not using firearms, may not be aware when they are transformed into combatants. These individuals could be charged, just like soldiers in uniformed service. Such are cyber hackers, drone users, etc., who, by contributing to the domination of one side over another, can be charged with war crimes. The advancements in military technology, particularly in the realm of cyber warfare, are viewed very positively for the ability of a "cyber" device in the hands of responsible persons or states. These special capabilities of these technological devices significantly reduce the costs of human lives in a traditional warfare.

With the advancement of technology and artificial intelligence[17] that is accompanying the technology of warfare in general, it is clear that these rules of war no longer apply only to state actors, since the next target chosen as a target can also be a private company or person. The use of smartphones and the sending of locations, photos and videos of Russian installations in Ukraine by the local population is proving successful for the Ukrainian military. The Ministry of Defense of Ukraine invites its citizens to send photos, videos and locations of Russian aggressors, with the motivational slogan "Become a leader of Bajraktar drones directly from your smartphone". The Russian cyber battle in Ukraine has shown that "fake" war scenarios can spread rapidly and widely, thanks to the cyber technology widely used there. In response to Russian disinformation, a campaign was organized and operated by the Western allies in Ukraine, which "bombarded" the world media space with "truths".

The surprise and superiority provided by high military technology in the hands of an attacking party is a military element as old as war itself, which is likely to determine the fate of a battle or even the next war. The disadvantage that comes from technology also lies in the ability of adversary hackers, capable of generating new variants of malware within our system, manipulating attack targets, spreading propaganda, as well as implementing automatic self-destruct mechanisms. As a result of the wrong use of smart technology, the case of the use of smart phones by Russian soldiers was a "failure". At 00:01 on New Year's Day 2023, six rockets were launched at a Russian military troop in a shelter, killing 89 soldiers along with the regimental commander. The Russians admitted that "it is clear[18] that our military troops were discovered by the massive use of cell phones by soldiers, despite the fact that their use was prohibited. This "mistake" allowed the Ukrainian army to track the coordinates of Russian military personnel and hit them with missiles. NATO intelligence agencies shared these assessments with their Ukrainian counterparts,

[17] Artificial intelligence is defined as the capability of a computer or computer program to perform functions and reasoning, currently typical associated with the human brain and mind, which are assumed to be matched by 2030.

[18] In its press release on January 4, 2023, the Russian Ministry of Defense stated that the rocket attack that killed 89 Russian soldiers in Donetsk was caused by theuse of smartphones by the soldiers, whose location led to the discovery of tehir hideout.

who tehn cross-referenced and enhanced them with their own national intelligence sources and analysis. In real time, many pieces of the "Russian mosaic", were gradually assembled, providing a clearer picture.

Images from US space technology company Maxar and posts collected on social media showed a large and unusual gathering of Russian forces. These images, combined with classified data and HUMINT, led to the conclusion that Russia was soon preparing to launch an aggression against Ukraine, as the armament of Russia, thanks to the media, was carried out in the eyes of the whole world. While information about the capabilities of the enemy's personnel, equipment, combat technique, weaponry and infrastructure is relatively easy to gather, detecting and assessing the adversary's "intent" is not at all. To discover the intention of the opponent, one must think and act like him. Assessments by Western powers of "Putin's intent" predicted possible military aggression, based mainly on increased Russian military exercises throughout 2021, as well as Putin's patriotic "essays" published a few months before the attack. In April 2021, Russia conducted a "surprise check" of its southern and western deployments, under the pretext of "supposedly aggressive" actions by the United States and NATO allies in the region. "We are now witnessing the largest concentration of Russian forces on Ukraine's borders since 2014," declared Secretary of State Antony Blinken at a meeting at NATO headquarters in January 2022. The frontal attack caught some NATO allies, as well as members of the Russian government, by surprise. In January 2022, the United States released information on Russian subversion to the press. "Russia has directed its intelligence services to recruit current and former Ukrainian government officials to prepare for a takeover of Ukraine's government and control its critical infrastructure with a military invasion force,"- stated Blinken in his statement.

This message was further reinforced by the statement of the Foreign Secretary of the United Kingdom, Liz Truss, and the head of the UK Defense Intelligence, Lieutenant General Sir Jim Hockenhull, who in the press statement, on February 19, told reporters that: " ...To date, we have not seen evidence that Russia has withdrawn its forces from Ukraine's borders. The opposite is happening, Russia continues to increase military capabilities near the Ukrainian border."

The first recorded use of fully autonomous drones was used by the Israelis to locate, identify and strike Hamas militants[19].

On October 7, despite Israel's military being regarded as one of the best in the world, military and intelligence failures led to a significant loss of confidence. Hamas fighters used a combination of small arms and anti-aircraft missiles combined and supported with cyber technology. Hamas deployed electronic warfare drones to disable some of the Israeli military's mobile communications stations and observation towers along the border, preventing Israeli service officers from remotely monitoring the area through

[19] David Hambling,"Israel used the world's first fully AI-guided and operated drone", June 30, 2021.

video cameras. Moreover, the high-tech drones, part of the cyber war, destroyed the machine gun remote control system that Israel had installed along the wall, depriving the Israelis of a key means of fighting on the ground front. Cyber technology facilitated Hamas attackers to approach and blow up parts of the border fence and detonate it in some places with ease, enabling the attackers to create gaps that allowed thousands of Palestinians to cross.

The sudden "occupation" of more than 20 cities and Israeli army bases during that attack marked the worst breach of Israel's defenses in 50 years, destroying the nation's sense of security and confidence in its military. The strongest army in the Middle East proved powerless against a significantly weaker enemy, leaving Israelis defenseless for most of the day against squads of terrorists who killed more than 1,000 Israelis, including soldiers killed in their sleep, the kidnapping of at least 150 people, the occupation of at least four military camps and the spread of military actions across more than 30 square miles of Israeli territory. According to four senior Israeli security officials, speaking anonymously, "these military operational weaknesses were among a series of logistical and intelligence mistakes by Israeli security services that paved the way for Gaza's incursion into southern Israel." The consequences have been devastating for Israel's security, and has damaged its reputation as a reliable military partner in the region. Before October 7, 2023, Israel was a model of security issues for many countries in the region[20]. It is no longer an invincible state, but very vulnerable, and this was also demonstrated by the resignation of the head of military intelligence on April 20, 2024.

From a national perspective, it is the duty of each country to protect its own networks, since NATO lacks dedicated capacities for the cyber threat, relying instead on the combined capacities of the 30 member states. In 2023, NATO's competitors heavily invested in technology to gain advantages, including in armed conflict. This evolution warns that authoritarian states may indirectly develop cyber technology, disguising the true purpose behind the advancement of AI in civilian equipment to weapons of mass destruction. Artificial intelligence in warfare technology is regarded as a power multiplier of cyberattacks[21]".

2. Challenges of future wars with "proxy war", "army of none" and "false flag" operations

If the history of warfare offers insight into future trends, "proxy wars," "army of none," and "false flag" operations are expected to grow and dominate future wars. Given their high human, political and diplomatic costs, false flag operations are likely to remain undetected for extended periods. Placing these groups of mercenaries or "soldiers of none" calls into question the role of the "proxy war", as the past or the future of wars. Future wars are envisioned to center on battles fought in cyberspace, biologically

[20] https://www.zeriamerices.com/a/7579656.html

[21] James S. Johnson, researcher at the James Martin Center (March 2020)

enhanced soldiers, and autonomous systems capable of processing information and striking faster than human reaction time. At best, advanced technology acts faster than ever to save soldiers' lives; at worst, deploying new technology uncontrollably can have devastating long-term consequences. The evolution of warfare technology reshapes combat methods and the weapons technologies we will use, defining the role of soldiers in the future. The future of warfare appears to cyclically revive traditional methods and forms in contemporary context and interest.

In 2014, the Kremlin orchestrated a "false flag" operation for the annexation of Crimea, using so-called "little green men[22]", described as members of local "self-defense groups", who demanded that the territory of Crimea be returned to Russia. The Kremlin claimed that these individuals had acquired their weapons, clothing and military equipment from civilian stores and had been forced to flee the country, unjustly occupied by Kiev. The more limited the violence to achieve the goal of the operation, the better it will be. For example, Russia's "little green men" did not use mass violence in Crimea. Using only existing local Russian forces that were present in Ukraine, Russian conventional forces were able to enter Crimea in 2014, creating massive confusion as well as delaying any response. Within days, Russia "de facto" occupied Crimea, facing little resistance. Paralyzed Ukraine found itself powerless, while the great powers found themselves faced with a fait accompli, able only to respond with sanctions.

On September 24, 2023[23], Kosovo avoided falling prey to another "false flag" attack by Serbia, which in fact exposed the west the face of Belgrade´s unchanged stance since 1999. On October 4, 2023, Marija Zakharova, Moscow's spokeswoman, recycled the Russian narrative used before for the attack on Ukraine; the cause of the terrorist attack was "the ethnic cleansing of Kosovo against the ethnic Serbs in the north"!?. Vučić used the same "Russian book of excuses" for the attack in Bnjska on September 24, 2023, just like the Russians did with Crimea. Vučić described the Serbian mercenaries as local citizens revolted by the repressive Kosovar government, while the Serbian weapons and uniforms were "purchased from the free market". But unlike Russia, the Serbian government shelters, protects and decorates the killed terrorists, thus legitimizing the authorship of this act, which is actually a proxy and "false flag" operation gone wrong. In war materials seized by the Kosovo police, were found documents that prove the direct participation of Millan Radoicic in this action.[24], along with the bodyguard of Aleksandër Vulin, former director of the BIA, who are already on the US blacklist.

The real aim of the Serbian paramilitaries hiding in monastery seems to be the creation of a new, highly sensitive source of armed conflict in Kosovo. According to

[22] https://nacionale.com/politike/cka-jane-burrat-e-vegjel-te-gjelber-qe-i-permendi-kurti-ne-mediumin-britanik

[23] https://www.kosova-sot.info/opinione/691889/cka-ndodhi-me-24-shtator-2023/

[24] https://sinjali.com/n1-arrestohet-milan-radoiciq-i-caktohet-masa-e-paraburgimit-per-48-ore/

the "false flag" scenario, "Serbs sheltered in a sacred place (an Orthodox monastery) are attacked by the Albanian, even Muslim, police of Kosovo. Following this, the association would have its martyrs, perhaps even Orthodox clergy "killed by the Albanians". To damage Kosovo's reputation and put Pristina under accusation, the Serbian intelligence service BIA had planned a "false flag" to kill prosecutor Dick Marty[25], who has seriously and unfairly accused the KLA in the CJND. Since the 'hatred of Kosovars' towards the lying prosecutor was universally known, the murder would be easily blamed on Kosovo. Had this "false flag" operation gone undiscovered, it could have raised another unfair charge against Kosovo in favor of Serbia.

Moscow is expanding its influence in the region and among non-NATO and EU countries by strengthening commercial ties and engaging in frequent high-level visits, powerful information campaigns[26] and partnerships with local media, bloggers, and politicians that promote Russian-friendly news or anti-Western narratives. Russian corporate sponsorship of football teams[27], charity events, schools, athletic associations, and Russian language or cultural associations help foster goodwill among target populations. These soft power instruments emanating from the private sector constitute a large part of Russia's public diplomacy in the region, complementing the broader formal reach of the Russian state[28] through embassies, cultural centers, friendship societies, the church and honorary consuls.

Moscow-backed friendly media in the region eagerly highlight local grievances[29] against Brussels, Washington or Balkan politicians who push their countries too far west. These narratives often portray the West as the cause of the region's democratic shortcomings, economic troubles and ongoing ethnic divisions. They claim that US or EU support for certain pro-Western political elites is the main cause behind states' failures to tackle erosive corruption or develop political systems based on the rule of law and empowered civil societies.

'Proxy' distraction warfare operations are combat actions that mainly opposing armies use against each other to avoid the truth the attack, the intent of the situation and even the cause of an incident or war. The war in Ukraine is a proxy war, since the West is fighting the alliance Russia - China - Iran and North Korea on Ukrainian soil. This is proven as such when considering the immediate cessation of the supply of drones and artillery shells to Russia by China and Iran, as well as the cessation of Western aid to Ukraine. This would likely force the conflict to end and bring the parties to the negotiating table.

---

[25] https://balkaninsight.com/2023/12/28/dick-marty-author-of-explosive-kosovo-war-crimes-report-dies-at-78/

[26] https://www.nytimes.com/2018/04/10/world/europe/european-union-balkans.html

[27] https://www.gazprom-football.com/en/gazprom.htm

[28] http://www.kas.de/wf/doc/kas_51729-544-2-30.pdf?180306092933

[29] https://www.reuters.com/article/us-serbia-russia-media-analysis/on-serbian-airwaves-a-battle-for-heart-of-balkans-idUSKBN17Z0X1

Historically, ships at sea were not restricted from using false flags, and even today, warships employ such technique, so-called "deception operations", to approach enemy ships. Due to the difficulty of identifying flags at sea at great distances, particularly in poor weather, sailors could not identify ships with the correct flag, and as a result, false flags were very effective. A warship is occasionally allowed to display a flag of a neutral or even enemy nation in order to get as close as possible to a hostile warship before opening fire. This practice was known as military deception in an era when the effectiveness of warships' cannons was limited. Such conduct, and other similar acts of deception, were not considered illegal, as long as the ship displayed its true flag during actual combat operations.

In modern usage, a false flag operation is a calculated ploy designed to create the illusion of an attack on a state, providing justification for retaliatory military operations against the alleged offender. In addition to justifying wars, such operations undermine the credibility of adversaries and other relationships on the national or international stage by convincing others of the guilt of an action they did not commit. The success of such operations can drastically change a tactical or strategic situation, whether in economic conflicts between trading powers or even political opponents campaigning against each other in elections.

A cyber operation is a perfect "false flag" if the threat actor behind it will take steps to mimic or use another threat actor's special infrastructure, tactics, techniques or procedures. Unlike traditional domains such as land, sea, air, or space, this deception is prevalent in cybercrime and cyberwarfare, allowing perpetrators to masquerade as others to evade accountability. In addition to justifying wars, these "hybrid" cyber operations undermine the credibility of adversaries and other relationships on the national or international stage, convincing others of the guilt of an action they did not commit. The success of such operations can drastically change a tactical or strategic situation, whether in economic conflicts between trading powers or even political opponents campaigning against each other in elections.

The world of technology demands its integration into our academies and increased attention to emerging challenges before they escalate beyond control. Denouncing what is described as a "broken" relationship between the military and the public it serves, military planners and weapons technologists note the rise of the phenomenon of private armies or "army of none".[30] Artificial Intelligence, which generates new data, such as texts, images or design, which are used in "smart" cyber wars, as well as in all aspects of our lives, is expected to generate and enhance the speech synthesis, translation and automation critical for command and control (C2). ChatGPT is expected to make a revolution especially in the record processing of information and intelligence, as a basis for military decision-making. Increasingly sophisticated AI systems require processing and analytical power, which means an industry emphasis on future military technology. The speed of information processing and its data

[30] Paul Scharre; https://bukinist.al/sq/oferta-te-ndryshme/10652-ushtria-e-askujt.html

analysis is at a very high level that requires military personnel to be trained more quickly with enhanced capabilities for self-evolution.

AI experts may not understand the technology's implications on future warfare as a concern considering the speed of change, the entities wielding the technology, and its impact on military technology and warfare in general. The Cyber Defense Technical Agreement between the NATO Computer Incident Response Capability (now known as the NATO Cyber Security Center) and the Computer Emergency Response Team for EU institutions, bodies and agencies (CERT- EU) provides a framework for sharing information and best practices between emergency response teams.

At the 2023 NATO summit in Vilnius[31], the Allies committed to further seek to develop reciprocal and effective partnerships, involving partner countries, international organizations, industry and military academies. Recognizing the need for swift action, NATO also launched the Virtual Cyber Incident Support Capability (VCISC)[32] to support national mitigation efforts in response to significant malicious cyber activities. Meanwhile, our country and our Armed Forces continue to pursue, adapt and develop programs and establish innovation centers[33]. It is crucial that the new generation of military students be trained, stays informed and up-to-date with the news that science and technology brings to the Armed Forces of the Republic of Albania. Our adversaries not only develop technological capabilities, but also closely follow our steps[34].

Conclusions

The year 2024 and beyond is likely to witness an environment of increased "deniable" warfare as a result of (AI) and efforts to integrate it, both by NATO and other security institutions which require knowledge of technology.

Cyber operations, "proxy wars", clashes with "army of none" and "false flag" operations are expected to be the future of armed conflicts between states.

The private sector is confirmed to be a key player in the future of cyber warfare as well, where the consequences are expected to be crucial for NATO doctrines to respond more effectively to cyber threats.[35].

AI is expected to generate and enhance speech synthesis, translation and automation so useful for command and control (C2). ChatGPT, in particular, is expected to make a revolution, especially in the rapid analysis of information and intelligence, as a basis for military decision-making.

---

[31] https://www.evropaelire.org/a/agjenda-samiti-nato-kosova-jashte/32497257.html

[32] https://cesk.gov.al/wp-content/uploads/2020/07/Kategorite-e-incidentit.pdf

[33] https://www.kryeministria.al/qendra-e-inovacionit-te-sigurise-dhe-mbrotjes/

[34] http://www.panorama.com.al/rama-inauguroi-kendren-e-re-te-inovacioni-te-sigurise-dhe-mprodjes-reagon-rusia-kender-kibernetike-e-orientuar-per-sulme- to us

[35] https://www.cnn.com/2024/03/25/europe/ukraine-starlink-drones-russia-intl-cmd/index.html

As AI systems become increasingly sophisticated, they demand greater processing and analysis power, driving the industry toward advanced military technology. The speed of information processing and its data analysis is at a very high level that requires military personnel to be trained faster with enhanced self-evolution capabilities.

Current geopolitical affairs indicate that humanity is on the brink of a new "dawn," driven by future technologies such as AI and genetic engineering. While these advancements are expected to achieve rapid development, they also come with potential side effects for security[36].

The wars in Eastern Europe and the Middle East indicate we are facing a critical moment in geopolitics. The shift towards authoritarianism and the long-anticipated decline of the hegemony of Western democracy has finally happened.

References:

1. Caprile A.and Delivorias A., *European Union sanctions on Russia: overview, impact, challenges*, EPRS, European Parliament, March 2023.
2. Jon Harper, *Ukraine is an outstanding laboratory for military and AI studies*; August 1, 2023; see:https://defensescoop.com/2023/08/01/ukraine-is-extraordinary-laboratory-for-military-ai-senior-dod-official-says/
3. "*War*", USNI Proceedings, June 2023, https://www.usni.org/magazines/proceedings/2023/june/struggle-black-sea-russian-navys-frailty-russo-ukrainian-war
4. "*Russia delivers Black Sea ship warning as Ukraine decries 'hellish*" *port attacks*, Reuters, July 19, 2023, https://www.reuters.com/world/europe/russia-strikes-ukraines-Odessa-port-hellish-attack-official-2023-07-19/
5. "*Ukraine intensifies efforts to break the blockade of the Black Sea*", September 17, 2023, see: https://www.ft.com/content/ f2c8312f-feac-4d1d-983f-f1798258de9f
6. Paul Pedrozo, *The Russia-Ukraine War at Sea: Naval Blockades, Visits and Search, and Targeting War-Sustaining Objects*, Lieber Institute, 25 Aug. 2023, see: https://lieber.westpoint.edu/russia-ukraine-war-
7. Dominika Kunertova, *"The War in Ukraine Shows Game-Changing Effect of Drones Depends on the Game"*, Bulletin of the Atomic Scientists, Volume 79, 2023 - Issue 2, see: https://www.tandfonline.com/doi/full/10.1080/00963402.2023.2178180
8. "Prized Russian Ship Was Hit by Missiles," The New York Times, April, 2022, https://www.nytimes.com/2022/04/15/us/politics/Russia -moskva-ship-sunk-ukraine.html
9. Electronic resource: https://www.reuters.com/world/europe/ukraine-military-says-hit-zalyv-plant-port-city-kerch-crimea-2023-11-04/
10. Justin Bonk, *Russian Combat Air Strength and Limitations: Lessons from*

[36] https://www.the-coming-wave.com/

Ukraine, 17 April 2023, CNA Occasional Paper, https://www.cna.org/ reports/2023/05/russian-combat-air-strengths-and-limitations

11. A. Horton, R. Mellen, S. Granados & A. Galocha, These are the Western air defense systems protecting Ukraine, The Washington Post, 19 May 2023, https:// www.washingtonpost.com/world/2023/05/19/ukraine-air-defense- systems-patriots/
12. Mathew Luxmore, *Ukraine runs into Russian Air Superiority*, The Wall Street Journal, 17 June 2023, https://www.wsj.com/ articles/ukraine-runs-into-russian-air-superiority-82c621c
13. Ulrike Franke, *Drones in Ukraine and Beyond*, August 11, 2023, https:// ecfr.eu/article/drones-in-ukraine-and-beyond-everything-you-need-to-know/#:~:text=Drones%20have%20documented%20destruction%20,%20direct%20aid%20and%20performed%20strikes
14. Christian Triebert, Haley Willis, Yelyzaveta Kovtun, and Alexander Cardia, Ukraine's Next Counterstrike: *Drone Strikes on Russian Soil*, The New York Times, 31 July 2023,https://www.nytimes.com/2023/07/31/world/europe/ ukraine-drone- strike-russia.html
15. https://www.armyrecognition.com/defense_news_april_2023_global_security_army_industry/list_of_the_808_tanks_that_ukraine_will_receive_from_nato_allies_with_a_part_already_delivered.html
16. William A. Arkin, *How Ukraine Is Crushing Russia's Famed "God of War" Artillery*, Newsweek, 92 Aug. 2023, https://www.newsweek.com/russias-god-war-failing-1816722
17. Sebastien Philippe, The Emerging Technologies Arms Race, Nuclear Weapons and Global Security NASA Astrophysics-Data-System (ADS), 2021, https:// ui.adsabs.harvard.edu/abs/2021APS..APRY05003P/abstract
18. Max Hunder, Jonathan Landay and Stefaniia Bern, Reuters, 13 December 2023, https://www.reuters.com/technology/cybersecurity/ukraines-biggest-mobile-operator-suffers- massive-hacker-attack-statement-2023-12-12/
19. November 14, 2023, https://time.com/6334176/ukraine-clearview-ai-russia/
20. David Hambling, *Ukraine's AI Drones Seek, Attack Russian Forces Without Human Oversight*, Forbes, Oct. 17, 2023, https://www.forbes.com/sites/ davidhambling/2023/10/17/ukraines-ai-drones-seek-and-attack-russian-forces-without- human supervision/?sh=649dbc8e66da
21. Daisy Stephens, *If we fall, you fall: Fake video shows Paris attacked by Ukraine*, Independent, 12 Mar. 2022, https://www.independent.co.uk/tv/news/ukraine-paris-bomb-deep-fak
22. www.eprs.ep.parl.union.eu
23. www.europarl.europa.eu/thinktank

Security and its impact in regard to international relations

Lieutenant Colonel (R) Msc. Kristo RAPO
Military Scientific Research Institute

Abstract

Classical theories of international relations teach us that security is something that comes with independence guaranteed by sovereignty. Thomas Hobbes said that "the security of men is the supreme law" from which sovereign duties arise and from which it is dictated that governments are formed for the sake of peace and that peace is dictated for the sake of security.

Special security agreements are realized through institutions and practices of diplomacy, the terms of which are usually set out in understandings, agreements, minutes, notes, declarations, treaties, covenants and statutes. When diplomacy is insufficient to deliver the desired result, when a certain threat becomes intolerable and a negotiated solution seems impossible, then security is pursued through the activity of war. The great powers, more than any other political, economic, social, religious or cultural institution, are charged with the responsibility of determining their interests and, moreover, regulating policies for the sake of "international peace and security."

This is considered for minorities suffering from oppression of a majority, lack of self-determination, and thus membership in the society of states, offers the possibility of security.

Keywords: security, international relations, political system, sovereignty, security dilemma, rule of law, balance of powers**.**

Introduction

War and armed conflict has seriously affected the living conditions of large numbers of people in a very negative way throughout history. Security studies began as a way to overcome or reduce the consequences of armed conflict. So the importance of international security and its study cannot be underestimated. If one tries to improve the living conditions of all the peoples of the globe, then a very important aspect to consider is conflict prevention.

Faced with an increasingly complex and volatile strategic context, progressive forces in the world, particularly the EU and the US, are committed to strengthening security and stability by defending the rules-based international order, according to international bodies and as defined by the UN Charter. This can be achieved through crisis response, capacity building, especially for enhancing cyber security, providing humanitarian assistance, etc. The great powers, the middle powers, but also those with regional or global influence, must be responsible and useful actors for the security of the world. In today's changing geopolitical context, mutually beneficial security and defense partnerships are essential to upholding the rules-based international order and effective multiraterism, achieve common goals and contribute to peace and security worldwide. Cooperation between all bodies and partnership is a key pillar for the international security and defence agenda.

Through opening the pathways for dialogue and partnership as coherent, consistent and inclusive as possible, it should aim to maintain a high level of ambition in security and defence. It is time that through international bodies, forums, initiatives, agreements or treaties, evaluation takes place collectively in the context of geopolitical developments and security and defence partnerships. All together, politicians, senior decision makers, military representatives, civil society, thought leaders and opinion-makers should examine the trends, issues and initiatives in security and defence and how they can contribute to international peace and security.

It is already clear that all states and their governments must support and be united behind the rules-based international order and in unison with the United Nations at its core. It's something that unites everyone and orientates them, to continue to work at the core of the international system and not only to protect it but to make it even stronger. We all know that partnership is not an addiction, but it is a strength, so becoming a partner means being stronger. To benefit all parties, we must adapt our mutually beneficial partnerships in order to help us meet our international responsibilities. At the Schumann Forum for Security and Defence, Mr. Borrell said: "I want to send you a message: the European Union was established to solve the problems within Europe. The European Union came from the ashes of war, from a terrible war. Europe almost committed suicide. We were killing each other so much that in the end, we decided peace needed to be made - and we did (it)".[1]

[1] Address of the High Representative of the Union for Foreign Affairs and Security Policy Josep Borrel, delivered at the Schuman Forum for Security and Defence, March 2023.

Borrel also noted that the Cold War was over and the world became global. Now the European Union must accomplish something more than just make peace among Europeans, but be an actor in the world that can contribute to a better world. We want to become a stronger and more valuable partner within NATO if so, but also with the rest of the world, and with anyone who wants to contribute to a peaceful and prosperous world. We must take seriously the role of every nation or state, powerful, weak with or without influence, in the global world in which we are living, which is not the world of 1945, nor the world of the last century, but is completely different, and in this new world, we can and must do more and better, "Today and the years ahead."

1. Security, an essential value of human life, mutual obligation of the state and citizens

The term security is closely related to that of sovereignty. "Security" comes from the Latin Securitas, meaning freedom and derived from caution or safety. This word was conveyed in the Roman languages and then in English, with the same essential meaning completely intact. The most important meaning of "safety" is the condition that "you are protected or not exposed to danger"[2]. This implies being "free from caution, fear or anxiety or alarm," which is a sense of security or freedom from the absence of danger. Hedley Bull[3], regarding the essence of security for our purposes argues that "security in international politics means nothing more than security: either objective security, security that actually exists, or subjective security, what has been felt or experienced." It is a refuge and care in our relations with other people, who together with states make themselves safe by establishing armed forces, diplomatic contacts, and other arrangements aimed at protecting them.

First, we need to understand the idea of security as a core value of human life and its fundamental assumptions. To be safe, we must not be affected by danger or fear. The desire for safety is a protective and self-protective response to the fact or threat that we may be harmed by other human beings. If there were no menacing people, the need to guarantee safety would disappear. The four main assumptions underlying the idea of security are: safety in what, from what, for what and by what means. Issues of security and insecurity are integral to all issues related to problems and practices of ethnic diversity in a world of national states, including self-determination, borders, human and minority rights, ethnic cleansing, genocide and humanitarian intervention. These highlight the importance of security in international relations.

Just as physical survival is the primary issue of any individual, so is national security a primary issue of any state. Checking whether the home's entry door is locked before bed is the safety dilemma. The state, with its monopoly on the use of force, is one that cares for the order and tranquility of the citizens, while the anarchistic nature

[2] Taken from Oxford, English dictionary.

[3] Hedley Norman Bull, professor of International Relations at the University of Oxford.

of international politics makes states very uncertain on their own when it comes to the goals of other states. Thus, in the absence of a single world government and the presence of armed entities (states) which make autonomous decisions for war and peace, it arises that Jon Herc [4] calls a "security dilemma", which can be explained in this way: "The search for security by one state A produces uncertainty in another State B, Who, fearing the intentions of State A, takes measures to increase its security, but this only reinforces the uncertainty of State A and thus to infinity, and sometimes to absurdity! According to political science, the security dilemma is a situation in which actions taken by one state to increase its own security trigger reactions from other states. These reactions affect and result in a reduction, not increase, of the security of this state. With NATO membership, our country solves the security dilemma with its neighbors. Small Balkan states with ridiculous miniature armies would not be funny at all when they started fighting each other, solving through conflict their security dilemma. Thus, sitting at the joint table in Brussels, under the umbrella of America, Balkan countries cooperate and draft their own security plans.

Each country drafts national security policy, which is a document describing how a country provides security to its state and citizens, and is often presented as a generalized document. This document can also be called a plan, strategy, concept or doctrine and has a role for the present and future, as it outlines the country's basic interests and sets out guidelines for dealing with current or future risks and opportunities. They are in a hierarchy superior to other security policies, such as military doctrine, internal security strategy, etc., which deal with national security on the basis of specific agencies or issues. It is also distinguished from them by the range of topics it addresses and tries to chart both internal and external risks. Finally, it seeks to integrate and coordinate the contributions of national security actors in relation to the interests and risks considered most important and international.

Some countries, such as the United Kingdom, France and China have no separate, unified security policy documents, but rely on defence policies or "white papers" – draft policy documents that focus solely on national defence. Another part of states does not make these documents public or have comprehensive policies on security or protection written. It is imperative that states should have a comprehensive and detailed national security policy and the main reasons are:

• ensure that the government will deal with all risks comprehensively;

• increase the efficiency of the security sector by optimizing the contributions of all security actors;

• to guide the implementation of security policy;

• to build the internal consensus of the country;

• increase regional and international trust and cooperation.

[4] Jon H. Herz, an American international relations scholar who formulated the concept of the Security Dilemma".

For a long time, internal and external risks have been treated separately, but increasingly, security policies are including comprehensive assessments of both the domestic and international environment, formulated as a comprehensive framework, the product of an in-depth analysis of all risks to national security. This requires consulting all interested parties, governments related to security issues and it would be ideal if the contribution of the international and non-governmental sides were taken. These policies can help harmonise the contributions of the growing number of security stakeholders, including those at national level, local government, the business community (e.x., in defence of vital infrastructure), various civil society organizations, as well as regional and international institutions.

Political parties involved in national security should be guided by national security policy, which provides models for coordinating operational decisions with the short and long-term endpoints of this policy. Through the centralized process, the optimal use of resources is possible, avoiding inequalities, unnecessary things and omissions during design and implementation. By deepening discussion and cooperation along professional, governmental and party lines, we ensure the broadest application of security policy. This dialogue contributes to creating a consensus on core national values and interests, as well as the risks that challenge them.

National security policies are instruments for building trust at regional and international levels. A coherent and transparent policy communicates to the international community the concerns of the state regarding security, thus enabling international understanding and cooperation. The main challenges to national security policy are:

- Balance disclosure and secrecy. Some countries try to avoid this by using vague language (it's known as "strategic ambiguity"). Its contents should reflect the general security points, while the application of these should be left to secondary doctrines or other planning mechanisms.

- Be perceived as a conflict between the need to preserve freedom of action and the restrictions placed on the actions of leaders. Many states prefer to deal with specific issues rather than specific countries, while if a clear signal should be given to any country, it can be mentioned by name.

- Balance national security policy issues regarding their cost, either in human or material terms.

- To balance public debate with expert input, if there is a perception that the document has been captured by political interests, it could undermine its usefulness.

There is a mutual responsibility of the state and the individual. The citizen is obliged to take action to preserve a healthy society. These include helping law enforcement, raising healthy children, participating in social life, paying taxes etc. The relationship between the state and the individual is expressed in full protection of the latter by the institutions of state power, the security of the individual is protected by law. According to Hobbs, "The safety of men is the supreme law." In the modern period,

the idea of the highest value of rights and freedoms is to some extent declarative. The readiness of the state and society for practical implementation of the model of the legal state is determined in the constitutional consolidation of its basic principles, which indicates evolutionary development. The nature of the relationship between the state and the individual is the most important indicator of the security and conditions of society at large. The legal restrictions on the freedom of people and the actions in society are objective, therefore the state must define the limits of its interference in this area. Moreover, they are focused on the interests of the people themselves so that one person does not suffer from another person's freedom. It is important to clarify the mutual responsibility between the state and the individual. If a person is responsible for his actions, the most important function of the state is to protect their life, security, property and freedom. The contradictions must be resolved by impartial judicial bodies on the basis of a legal right.

Even in ancient times, the idea of building a rule of law and the security of the individual has disturbed philosophical thought, being in search of right forms of public life, despotic rule and absolutism. The problems of the formation and development of a legal state, its fundamental principles, relations between the state and society remain unresolved. Today, states aspire to join a single global community, built on mutual interaction and respect, which further increases interest in the issue of security and a rule of law for the development of common values of the individual and universal values for all states.

In this regard, a state of law, built on the principle of the rule of law, which is considered the highest priority, changes the definition to: "The establishment of a system of political, legal, civil and public guarantees guaranteeing the validity of constitutional provisions, mutual responsibility of the state and of the individual constitute the process of forming the rule of law"[5]. This leads to the emergence of a new relationship between the individual and the government, which is fundamentally different from an autocratic state. Civil society, where free citizens are united, represents a social basis for a state of law. It realizes a person's individual rights and freedoms, creative work opportunities, supports and provides pluralism of opinion. "The transition to a rule of law from totalitarian methods is accompanied by a sharp and intense reorientation of the social activity of state power"[6].

The basis of a rule of law are the principles of justice and humanism, the equality of individual rights and freedoms. This state, exercising the supremacy of power and its exclusiveness, realizes the full assurance of the freedom of public relations, based on equality and justice for all citizens, guaranteeing their security. A well-governed national state is a secure security organisation. It was this reason that he eventually replaced clans, tribal societies, fiefs, free cities, medieval esnafs, duchy, dynastic states and even empires, to become the basic form of modern political organization.

[5] Afanasev, S. A. (2017) *Political rights and freedoms*.

[6] Avdeev, D. A. (2017) *Constitutional and municipal law*, 3.

In this sense the term "national security" refers to all those public policies through which the national state ensures its survival as a separate and sovereign community, thus making it the security and prosperity of its citizens. The mutual obligation of security between the national state and its citizens is the normative basis on which the claim of the national state to be the defender of the people is justified. However, for the national security model to be true, the coercive power of the state must be used as a last resort and as rarely as possible.

2. Security from the standpoint of international society and the role of the great powers

International security aspires towards the achievement of a general condition of peace, order and legality within the society of states. The history of international society is presented as a constant struggle with problems of disorder and insecurity as its companion. In practice, the primary responsibility for providing international security lies with those states we refer to as great powers. Their role will be assessed by the balance of power and the concept of great powers. A recurring problem is ensuring that all major powers remain and play the role of good international citizens, acting to uphold, not subvert, international law and the balance of powers. When a great power begins to act as an intruding or outside international law, security is jeopardized and the potential for war increases. These are treated as fundamental international security constraints in the context of military intervention, nuclear non-continence and climate change.

The main organisational principles such as sovereignty, formal equality, independence and non-intervention in domestic affairs, which still govern the international society of states, were laid out in several treaties joined together as the "Peace of Westphalia" in 1648.[7] However, some states have always been more privileged than others. Among the nearly 200 states of the early twenty-first century, some are the largest regional powers while some are fairly small countries. Historically, small states rarely exert great influence on world affairs and have often not even been free to choose their own historical path. In cases where small states are influential in international relations, they are usually in a negative sense: they rose to prominence whether they were subject to aggression or competition between major powers, or hostages to the regional balance of power sharing by major powers. Many of them are historically interesting and important in themselves, and some play important roles in regional issues. Yet despite the political trumpeting that the histories of all nations carry equal moral weight, the truth remains that they are not the axis around which world history and international relations revolve, but rather it is the great powers that define them, whether acting separately or together. For the same reason, key ethical considerations pertaining to international security issues have been and remain the domain of the largest and most powerful states.

[7] This agreement was achieved in the cities of Osnabruck and Münster of the Westphalia region, Germany.

The term **"great power"**[8] means a sovereign state that is recognized as a state, which has the capacity and expertise to exert its influence on a global scale. These states possess military and economic strength, as well as diplomatic influence and compelling opportunities, which can lead to the point where medium or small countries consider their own opinions before taking their own decisions or actions. According to international relations, the status of the "great powers" can be characterized in the powers of power, its spatial aspects and dimensions. This status may be formally recognised at conferences such as The Vienna Congress, or an international structure like the United Nations Security Council (China, France, Russia, the UK and the US are five permanent members). It can also be recognised unoffitively at a forum such as the G7, comprising Canada, France, Germany, Italy, Japan, the UK and the US.

The **middle power** in international relations is a state whose position on the spectrum of international power is in the middle, i.e. that of the great powers, but with sufficient capacity to shape international events.

Weak power or dependence on foreign states, are the states in the global power structure that are economically supported by the strongest countries, allowing them to exercise significant control over their economic and political behavior. This encourages underdevelopment, adoption of policies for the interests of a stronger country, which can hinder domestic growth, accelerate environmental destruction, or create temporary growth that excludes sustainable development and economic independence.

Cathal J. Nolan[9] has examined the relations of security and great powers, which despite a doctrine of "radical state equality" that appeared hastily during decolonisation, still form "the axis around which world history and international relations revolve." Consequently, security questions are answered by referring to the interests and values of these former among equals, because power is still the principal currency of international relations. Nolan argues that a new U.S.-initiated international security ethic has evolved into a "rough consensus around a modified liberal internationalist view, a more cautious Wilsonianism, which sees long-term national and international security as achieved by progress toward a confederation of interdependent and free societies." Yet the biggest threat to this consensus comes not from an America vitalized by a muscular foreign policy of "regime change" but from an autocratic Russia and an enigmatic China. He concludes by arguing that it is the primary obligation of these Asian giants, as is the great powers, to fix their homes and therein spare the world from the calamities that usually accompany the decay and even the eventual collapse of unlawful regimes.

The Vienna Congress and the system of processes to which it led, was a real turning point. It is marked as the first of four major efforts in modern international history to

[8] The term "Great Powers" was first used in a treaty, only in 1815, at the Congress of Vienna..

[9] Cathal J. Nolan is director of the International Institute of History at Pardee School of Global Studies and Professor of History at Boston University.

to support the cooperation of great powers in peacetime, in achieving a better opportunity for international relations through continuous consultation and decision-making based on general agreements and principles of international justice. In each of the three previous attempts (1815, 1919-20 and 1944-45), victorious alliances composed of extremely diverse and often hostile major powers sought to expand wartime co-operation habits into the postwar period. They did so not only to shape and control the geopolitics of the postwar world, though this motive certainly was present, but also to build a more orderly and legitimate international society. Whenever such a thing was attempted, they failed to support their efforts, clashing over territorial or ideological differences, or falling prey to the bitter revanshism of some other major powers left out of consensus by the fall, or for ideological reasons still unreconciled with the idea of partnership.

In relations among great powers still dominate the essential ethical considerations of international security, because power as a motive and driving force in the affairs of states and nations retains an all-important importance and remains central to the achievement of international security agreements. With the end of the Cold War and the apparent triumph of liberal international ideas about security, partly in fact and globally in rhetoric in international law, reality still shows the struggles of power conflict between discrete political communities (states). With the turn of the twentieth century there is an unspoken consensus among the great powers on their fundamental international obligations. The main principles of this consensus are:

- To maintain a sound political and social order within their national boundaries, which, given their large size, encompass much of the world.
- Maintain political order in their regions, if necessary and by military intervention, or what used to be called their "spheres of influence" or even "their domains".
- To cooperate to maintain an international security order that respects the sovereign rights of all members, but increasingly recognizes a limited right of international investigation and even collective intervention, to mitigate human consequences and to block aggression by states threatening to use weapons of mass destruction.
- Respect and transcede the principal body of international law towards oneself (d.m.th, obligations between members of the society of states).
- Uphold and adhere to the core principles of international law, ensuring the fulfillment of obligations between members of the global community of states.
- Promote free trade as a fundamental driver of mutual prosperity and a key pillar for achieving sustainable international peace and stability
- Provide humanitarian aid in times of overwhelming national disasters or in countries where "failed states" or genocidal regimes cause severe humanitarian crises.
- Foster international cooperation in addressing pressing global challenges that cannot be resolved by any single nation or region acting alone.

Maintaining a just and stable internal political and social order stands as one of the foremost responsibilities of great powers. Evidence suggests that internal stability not only underpins the development of political, social, and economic relations within a country, but also serves as the most significant contribution a state—particularly a great power—can make to international security. The United States and the United Kingdom, historically the most stable and successful domestically, have been at the forefront of advancing a new international ethos of cooperative security. Today, the states recognized as great powers include China, Japan, Russia, and the United States. However, India—despite facing challenges such as internal conflicts, outdated economic policies, and tense relations with neighboring countries and key nuclear rivals—should also be considered a rising power. While this list may evolve with time, it represents a reliable snapshot of the current global landscape amid a period of significant uncertainty and transition.

Numerous questions and concerns persist regarding the governance of the great powers. The United States' retreat from its traditional role as a global stabilizer, coupled with policies such as "regime change" and "liberate and leave"—regardless of their ultimate success—are unlikely to alter the broader patterns of international diplomatic and political engagement. These patterns have been shaped by the significant conflicts of the previous century, both hot and cold wars, as well as by diplomatic norms and visions rooted in stable leadership and the enduring influence of the U.S. military and economic power.

First, the most pressing and controversial issue today is Russia, a significant disruptor of international security since the latter half of the 20th century and beyond. Post-Cold War Russia remains an internally unstable and profoundly unjust society. Instead of transitioning into a market-based system capable of integrating its Soviet legacy, it devolved into a kleptocracy, where the nomenclature and security services formed alliances with traditional criminal networks to exploit the remnants of the collapsed Soviet system. While Russian leaders outwardly and rhetorically present themselves as democrats, their actions echo Soviet-era tactics, including stoking racism and xenophobia among the population. Moreover, this strategy extends beyond Russia's borders, with renewed interference in the domestic affairs of neighboring states. Russia's corrupt and increasingly autocratic political system prevents it from engaging meaningfully in any cooperative security framework established by other European nations. Given these realities, the international community has limited options. Its primary role is to support and safeguard emerging democracies in the region from illegal Russian political interference.

Russia continues to view the West as an "existential threat." Recently, it unveiled a new strategic doctrine, which, according to President Vladimir Putin, was necessitated by the "current upheavals in the international arena." This strategy is framed as a response to what Moscow perceives as "existential threats" to its security and development posed by the actions of unfriendly states. In line with this shift, Russia has officially designated 20 countries as "unfriendly," including the United

States, Germany, the United Kingdom, and Poland. Meanwhile, China and India are recognized as key allies of Russia on the global stage.

Second, at the dawn of the new millennium, one of the central security questions is the future trajectory of China. The key concern is whether China's ruling elites can adapt their political theory and institutions as effectively and swiftly as they have adapted their economic policies. This question is of profound importance for global stability. If China tries to emerge as a prosperous, broadly democratic (or at least more politically modern and representative) great power, it could significantly strengthen the security structure in Asia and the broader international system. The direction of China's foreign policy in modern international relations is shaped by the geopolitical legacy of its history and its long-term strategic ambitions—factors that transcend the policies of individual leaders. An equally important influence is the foundational structure of China's political and economic system, which defines the parameters and dynamics of its foreign policy. From its strengthening military capabilities and assertive actions in the South China Sea, to its involvement in nuclear proliferation, partnerships with autocratic regimes, and connections with terrorist organizations, China has long been considered a "systemic competitor." However, it is now viewed as presenting a "systemic challenge." China's expanding partnership with Russia, and Russia's growing ties with Iran, particularly following the invasion of Ukraine, are developments of increasing global concern. The current tensions in the Indo-Pacific region could have far-reaching consequences for global security, potentially even greater than the conflict in Ukraine. While Russia remains the most immediate and acute threat, what has shifted is the recognition that the outcome of the war in Ukraine is now intricately linked to the broader prospects for collective international security.

In terms of security, an armed attack across a state's internationally recognized borders is perceived as a direct threat to both human and national security, particularly for those whose homes and livelihoods lie in the path of invading forces or become targets of aerial bombardment, whether intentionally or as collateral damage. In this context, the most significant global event today is Russia's aggression against Ukraine, marking the most important development in European politics since the end of the Cold War. Nearly two years into the conflict, the actions on the ground, as well as the surrounding propaganda and disinformation, are starting to reveal more clearly the underlying causes and motivations driving this war.

In political science, particularly within the field of international relations, one approach to understanding the costs of conflict is to quantify the value of lost lives, the destruction in Ukraine, and the economic inefficiencies in terms of territorial gains or loss. While this may initially sound unconventional, it reflects a broader analytical tool used in geopolitical studies, where territorial divisions are often framed as a means to avoid or resolve conflict. This approach is not unique to war; similar cost-benefit analyzes are applied in other areas of international relations. The reason this kind of analysis is relevant today is that, in many instances, wars have become

less frequent due to the growing recognition that negotiation and compromise can offer more beneficial outcomes than the devastation of armed conflict. However, to fully understand why a war occurs, we must focus on why the parties involved were unable to reach a negotiated agreement by breaking the process down into two essential stages:

- First, we must define and discuss the core issues for which these two countries are willing to fight.
- Second, we must identify and examine "negotiation disagreements", that is, what prevents them from reaching one of the negotiated agreements.

The simultaneous existence of both is a prerequisite for war. If we have elements of one without the other, there is no war. Therefore, for war to occur, the coexistence of elements from both group a and group b is necessary. Fundamentally, this suggests a recurring pattern, which is troubling. It implies that wars are likely to persist for extended periods, with their resolution often requiring the military defeat of one side.

- The aggressor is defeated and cannot achieve his goal.
- The attacker achieves the objective and militarily defeats the other side, to the point where the defender can no longer attempt to retake it.

Both scenarios are possible between Ukraine and Russia, but ultimately, only one will come to pass. Ukraine has shown remarkable courage in its actions, yet it lacks the military strength to invade Russia and completely dismantle its armed forces. While Russia may possess the capability to inflict significant damage on Ukraine, the challenges faced so far make a decisive military defeat seem unlikely, as such outcomes are rare in this type of conflict.

Another way the war could end due to fundamental causes is through a dramatic shift of its objectives and priorities, where the original reasons for the conflict no longer apply. In this context, it is highly unlikely that Zelenskyy would suddenly abandon his claim to certain parts of Ukraine or agree to relinquish them. Similarly, it seems improbable that Putin would suddenly lose interest in seizing and holding specific territories or regions of Ukraine. What is more likely, however, is that Putin could be forced to withdraw, and this scenario aligns with the broader U.S. strategy to shape the outcome of the war.

Staying within the context of the topic, it's important to note that a war doesn't always have to end with a military defeat. Sometimes, the root cause of a conflict arises from long-term shifts in the balance of power. If we were to halt these changes in power today, the balance tomorrow would likely resemble the one we have now, and we could be less concerned about the future. However, this particular conflict remains unpredictable, and the eventual outcome cannot be clearly foreseen at this point.

3. Individual security in international society

The vision of a global human community that transcends international borders and prioritizes universal human rights over the interests of individual states or groups of states has noble roots in international relations. Within the framework of human security, which aims to protect universal human rights, humanitarian law, and the doctrine of the responsibility to protect, there are inherent limitations. These limitations stem directly from the reality that international relations are still structured around the principles of state sovereignty and pluralistic values.

The term "international community" is often used in geopolitics and international relations to describe a broad group of people and governments worldwide. To create an ideal society, it is necessary to reassess its foundational principles, identify the key components that drive social movements, and chart a path towards realizing a future global human community. Menno Boldt lays out the nature of globalization and challenges the dominance of Western democratic ideals and constitutional human rights, highlighting their limitations in fostering a better society. He offers a refreshed vision of society in the global age, one shaped by globalization, where all people can achieve humanity through global freedom, social justice, and universally recognized human dignity.

The global era, in contrast to previous social orders, has its roots in capitalism and is marked by globalization—a doctrine and system of social order driven by economic and utilitarian imperatives. The phenomena of globalization emerge from the reconstruction of the geopolitical landscape, influenced by economic, political, and cultural interdependence. To create a just society, it is essential to understand the interplay between these three areas and the roles of power, authority, and history. The United States plays a significant role in shaping the global era, and its actions have profound implications for the future global order. The fundamental components of social order—authority and relational social values—hold the potential for creating stable and predictable relationships, as well as the capacity to either humanize or dehumanize these relationships. Social orders in the modern era reflect the evolution from religious doctrines, divine rule, and law to the development of secular governments and the rise of sovereign nation-states. In each case, all three components are involved in the construction of ruling hegemony and the promotion of human dignity and human rights in the global era.

The social order authority on human rights has evolved from a moral framework rooted in church states—defined by a synthetic order based on religious doctrine—to a liberal democratic model primarily based on secular, legal systems for human rights. Globalization calls for the expansion and universal application of global rights grounded in human dignity. As the world transitions from sovereign states to a more interconnected global system, we will increasingly rely on interdependence and demand a social order founded on universally understood human rights. However, this vision can appear overly idealistic /quite saccharine. As globalization

advances and we move toward a global state, capitalism—if it continues on its current trajectory—aligns human rights and human dignity with utilitarian economic imperatives, further advancing the human rights of societies that accept capitalist hegemony. In this context, these virtues can be achieved through a global moral social order embracing transcendent humanity.

The Universal Declaration of Human Rights was drafted in response to the most egregious violations of human dignity, particularly after the horrors of the Holocaust during World War II. Its focus centers on the individual, and its preamble emphasizes "freedom from want and fear". The concept of human security aligns with this approach, as "most threats to human security directly or indirectly highlight the dimension of human rights." Its goal is to protect human rights through conflict prevention and by addressing the root causes of insecurity, ultimately fostering a global political culture rooted in human rights. In this context, human rights education becomes a crucial strategy for achieving human security. It empowers individuals to seek solutions to their problems grounded in the universal system of global values, supported by the rule of law and human rights, rather than relying on power or force.

Human security is promoted in society in a decentralized manner, beginning with the fundamental needs of both women and men, which include personal security, poverty alleviation, the fight against discrimination, social justice, and the promotion of democracy. True freedom from exploitation and corruption can only be achieved when people refuse to tolerate further violations of their rights. Civil society institutions, such as Transparency International, play a vital role in supporting emancipation processes by promoting human rights awareness. These institutions provide the essential foundation for human development and security. There are several key connections between human rights and human security. Personal, social, and international security are all aligned with established human rights frameworks. Security policies should be more closely integrated with strategies that promote human rights, democracy, and development. Human rights, humanitarian law, and refugee law provide the normative foundation for the human security approach. When these rights are violated, they represent significant threats to security. As such, they serve as crucial indicators for early warning systems and conflict prevention. Additionally, they play a critical role in the post-war period, supporting conflict management, transformation, and peacebuilding efforts.

Through the transfer of knowledge, skill-building, and behavior shaping, a genuine culture of prevention in human rights is established. Human rights are not only essential for conflict prevention but also form the core of governance and democracy building. By fostering active participation, increasing transparency, and ensuring accountability, human rights provide the foundation for addressing both social and global challenges. Governance is understood through two complementary forms of capacity-building: "state building" and "society building." The former contributes to "democratic security," which becomes particularly evident in post-conflict rehabilitation and reconstruction efforts. The latter, "social development, involves

extensive human rights education aimed at empowering individuals to claim their rights and respect the rights of others."

Human security is essentially an effort to build a global society where the security of the individual is at the center of priorities and international standards for human rights and the rule of law are framed in a coherent network for the protection of the individual. Building a community with a shared future for humanity demands the active participation and cooperation of all nations and peoples. This entails embracing diversity and acknowledging the intrinsic value of different cultures and civilizations, working together towards common aspirations. The spirit of solidarity and mutual cooperation are the cornerstone elements—without which the collective destiny of mankind cannot be realized.

The promotion of peace, security, and stability, along with addressing other global challenges, can best be achieved through collective effort, underscoring the need for solidarity and, above all, a deep commitment to shared goals. The formation of a community with a common destiny for humanity is rooted in the recognition of interdependence and mutual influence. Nations and peoples are intricately connected, and their futures are shaped by, and require, coordinated action in the face of global challenges such as climate change, pandemics, and terrorism. However, building the foundation of mutual trust and solidarity between peoples is often a complex and difficult task. Among the key mechanisms for strengthening cultural and educational ties between nations and peoples, the following are particularly significant:

- Encouraging student and academic exchanges.
- Supporting cultural events and programs.
- Promotion of language learning.
- Support of international research and scientific collaborations.

Albania can also contribute to the concept of a community with a shared destiny for humanity by actively promoting international cooperation and solidarity. This begins with strengthening ties, particularly with its neighbors, and extending these efforts to the broader international community, while actively supporting initiatives that promote peace, security, and sustainable development. Given the ongoing challenges in the Western Balkans—such as political instability, economic underdevelopment, and ethnic tensions—Albania has a key role to play in fostering regional stability and integration. Through these efforts, a better future can be built for all people, both in Albania, the region, and across the globe.

4. Clash of national, international and human security values

National, international, and human security represent a "clash of values" for which no permanent solution exists, despite the fact that each form of security may appear more compelling at times. These security paradigms remain inherently incompatible, as the demands of one often conflict with the demands of another, forcing us to

choose between them. National security has long been a central focus in political discourse, often prioritized over economic, social, and other aspects of societal well-being. However, the safety and well-being of the individual should take precedence over the narrow concerns of an elite focused solely on the sovereignty and territorial integrity of the nation-state.

Security studies, as a sub-discipline of international relations, lie at the very heart of the field. The discipline was implemented at Aberystwyth in 1919, motivated by the desire to learn from the lessons of the First World War and prevent a recurrence of such catastrophic events. Security remains one of the most discussed issues, both in high-level policy debates and in public discourse. The survival of key actors, primarily nation-states, has often been used to explain their behavior in the simplest terms. "No other concept in international relations can pack the metaphysical punch, nor command the disciplinary power of 'security'. Achieving consensus within security studies typically centers on threats to survival. While war and the potential use of force remain important components of the security equation, they are no longer exclusive. The definition of security has evolved to encompass a broader range of threats, including pandemics such as HIV/AIDS and COVID-19, environmental degradation, direct violence, terrorism, and interstate conflict.

For much of the 20th century, interstate conflict dominated security studies, particularly during the Cold War, and is now considered a sub-discipline known as strategic studies. Traditionally, the state was seen as the primary referent of security, with military force being the main tool for ensuring its safety. However, alternative approaches have emerged, broadening the scope of security studies to include a wider range of referents and threats. This expansion has created a blurred boundary between security studies and international relations, particularly as a result of globalization. "A nation is often considered secure when there is no threat that would force it to sacrifice its core values to avoid war, and when it has the capacity, if challenged, to preserve these values through victory." National security, in this traditional sense, is the ability to face and withstand external aggression. Although traditional approaches to state security continue to dominate, they are increasingly being challenged by new theoretical perspectives. These alternative approaches are persuasive not by ignoring traditional views, but by fully acknowledging and incorporating them into the evolving security discourse. The alternative perspectives on security not only focus on the nature of threats or their consequences but also emphasize the search for solutions to these challenges.

The evolution from traditional to non-traditional security issues is largely shaped by the strategies adopted by the West after the Cold War, particularly the implementation of the "preventive use of force," coercive diplomacy, and the increasing reliance on imposing diplomatic measures. Central to this shift has been the expanded role of intelligence in defining security threats, especially in the context of events like the 2003 Iraq invasion, actions following the September 11 attacks, and concerns over weapons of mass destruction and various forms of terrorism (religious, ethnic,

ideological). In parallel, a range of non-traditional security threats have emerged, which are now prominent on national security agendas. These include pandemics such as HIV/AIDS (which claims, on average, three times more lives each day than the number of people killed on September 11, 2001), the identification of drugs as national security threats, human trafficking, the flow of money, and the connections between organized crime and terrorism. Moreover, the role of children in conflict has become a significant area of concern for many countries. These non-traditional security issues have prompted changes not only in the security priorities of many nations but also in national legislation and the goals of international organizations.

Conclusions

The formulation of security strategies is a critical institutional process, aimed at maximizing the use of all available resources to effectively fulfill security missions. The dynamic nature of the security environment, which continually influences the prioritization of global challenges, necessitates a flexible and adaptive approach. Security organizations must strive to remain agile, constantly evolving their methods and practices to enhance their effectiveness in addressing emerging threats. To address the complex security challenges of the new international system, and to develop a comprehensive understanding of the analytical concept of security, it is essential to clearly define the key actors involved. These actors, who may simultaneously be the perpetrators and the victims of security threats, must be identified in relation to the various levels of security they are affected by:

- Security for the Individual (Individual Security).
- Security for the Social Group, Community, "Nation", Entity (Social Security).
- Security for the State or "Nation" (National Security).
- Security for the Region, that is, a coherent security region (Regional Security).
- Security for the Community of Nations or "International Society" (International Security).
- Security for the Globe or Planet (Global Security).

The new strategies include all aspects of the activity of security organizations and institutions and enable evaluation and planning of capacities for achieving the mission and objectives outlined in the relevant documents on national, international and human security and other strategies closely aligned with the specific priorities and areas of focus.

In fulfilling the mission, national and international organizations must provide objective, qualitative and useful information in time to enable decision-making on risks and threats from outside and inside, to the interests and national security of the country, allied countries, regional and international. Based on the National Security Strategy, all national and inter-institutional strategies, international commitments of the country, responsibilities in fulfilling the mission are drawn up, in accordance

with the needs of political decision-making and the contribution of law-enforcement institutions, for national security, as well as commitments in the contribution to international security.

References:

1. National Security Strategy of the Republic of Albania, approved by law no. 103/2014.
2. J. Jackson-Preece, Security in International Relations, 2011.
3. William Bain, The Empire of Security and the Safety of the People, London, 2006.
4. Cathal J. Nolan, Greenwood Encyclopedia of International Relations, Westport, CT: Greenwood Pub, 2002.
5. Sasson Sofer, The Courtiers of Civilization, Albany: State University of New York Press, 2013.
6. Radomir Compel&Rosalie Arcala-Hall, Security and Safety in the Era of Global Risks, 2021.
7. Adam Winkworth, Is the Security Dilemma Still Relevant in International Relations? 2012.
8. https://www.nato.int/
9. https://www.osce.org/
10. https://www.dcaf.ch/publications/documents
11. http://www.un.org/secureworld/report2.pdf
12. https://www.london.ac.uk
13. https://www.rug.nl/masters/international-security
14. https:/hdr.undp.org/doc/training/oxford/reading/fukuda
15. https://www.id21.org.
16. https://www.humansecurity-chs.org

Military strategy in a rapidly changing geopolitical reality

Colonel (R) Msc. Arben DHULI
Head of Section in the Military Scientific Research Institute

Abstract

Taking into consideration the latest developments and the two basic documents "National Security Strategy" and "Military Strategy of the Republic of Albania", I have tried to address in this article, from my point of view, strategies of some partner states, but also the strategy of countries that approach it differently in terms of perspective and importance, as well as the geopolitical situation.

Also, this article highlights the importance of the National Security and Military Strategy, which as regards their content, have specific issues that evaluate specific aspects and provide guidelines for taking measures to deal with critical situations, both internal ones and real and expected threats at the time of preparation, including the states of the alliance but also its opponents.

But let us see how these strategies are treated at a general level. At a national level, strategic culture reflects a set of society's values which owe to the use of force. At a military level, a nation's strategic culture or "methods of warfare" is an expression of how a nation's military will fight wars.

The geopolitical reality and the use of military force, such as the unjustified Russian aggression against Ukraine, has significantly changed the security paradigm. The strategy directs the activity of all public institutions with authorities and structures responsible for national security and defense.

In its entirety, the Military Strategy is a fundamental document through which the aims, objectives and main concepts for the operation and development of the Albanian Armed Forces (AAF) are defined. This is based on the Constitution of

the Republic of Albania and the National Security Strategy (NSS), drafted with comprehensive expertise.

As a strategy of a NATO member country, it is in harmony with the documents, concepts and processes of the Alliance where security and defense are part of collective defense. Developments in the strategic security environment have highlighted new challenges and risks of a geopolitical, hybrid and military nature, which are overlapping risks and threats such as: terrorism, violent extremism, organized crime, cyber attacks, illegal immigration, and health security.

The Black Sea region is of strategic interest not only for Romania, which I have taken as a case study in this study, but it is vital for European and transatlantic security.

Keywords: Strategy, concept, geopolitics, strategic culture, NATO, long-term development plan.

1. A nation's strategic culture and Military Strategy

A nation's strategic culture derives from its geography and resources, history and experience from its society and political structure. It represents an approach that a given state has successfully established in the past, while seemingly invariable it tends to develop slowly. It is no coincidence, for example, that Britain has historically favored sea power and indirect strategies or traditionally against maintaining a large military. Likewise, Israel's lack of geographic depth, its small but educated population, and technological knowledge have produced a strategic culture that emphasizes strategic development, diverse operations, initiatives, and a growing and evolving technology.[1] Australia's minimal geopolitical status, continental rather than maritime identity, and formative military experience have shaped its war path.[2]

A definition states: "Military Strategy is a set of ideas implemented by military structures to pursue desired strategic goals. The origin of the word "strategy" comes from the Greek language "strategos" and this term was used for the first time during the 18th century, in its narrow sense as "the art of the general" or "the art of arranging" the troops, as it deals with the planning and conduct of campaigns, the movement and availability of forces, and the deception of the enemy. Furthermore, the father of modern Western strategic studies, Carl von Clausewitz, defined military strategy as "the use of battles to win the end of war." BH Liddell Hart, placing less emphasis on warfare, defined strategy as "the art of deploying and applying military means to accomplish political ends," prioritizing political aims over military objectives.

[1] Michael I. Handel, The Evolution of Israeli Strategy: The Psychology of Insecurity and the Quest for Absolute Security, in Williamson Murray, MacGregor Knox, and Alvin Bernstein, eds., The Making of Strategy: Rulers, States, and War (Cambridge: Cambridge University Press, 1994).

[2] Michael Evans, The Tyranny of Dissonance: Australia's Strategic Culture and Why of War, 1901-2005 (Canberra: Land Warfare Studies Centre, 2005).

Even the military strategist Sun Tzu, who is often considered the father of Eastern military strategy, greatly influenced the historical and modern tactics of Chinese, Japanese, Korean, and Vietnamese warfare. His book "The Art of War" grew in popularity and saw practical use even in Western society. It continues to influence many competitive endeavors in Asia, Europe, and the Americas, including culture, politics, and business, as well as modern warfare.

Operations and tactics are the art of organizing forces on or near the battlefield to secure objectives as part of a broader military strategy.

The United States is the most powerful nation in the world and will be so for a foreseeable future. The way the United States operates affects not only its citizens, but also the world around it. Understanding the strategic culture of the United States is important to society, enemies, and those who are neutral. As a nation, America's strategic culture is shaped by loose security and filled with hatred of exceptionalism.

Strategic culture is that set of shared beliefs, summaries, and ways of behaving, derived from shared experiences and accepted (oral and written) narratives that shape the collective identity and relationships of other groups which determine the appropriate definitions and means to achieve security objectives. In this regard, Colin S. Gray stated: "...culture refers to the ways of thinking and acting in respect of the force, derived from the perception of the national historical experience, the aspiration for self-characterization... and from all the distinguished experiences of America (from geography, philosophical politics, civic culture and "lifestyle") that characterize an American citizen[3].

National strategic culture, both geographic and historical, have shaped America's national strategic culture. For most of America's history, North America's insularity and weak neighbors to the north and south combined to achieve the loose security of the United States. Protected by the Atlantic and Pacific Oceans and the Royal Navy, the United States grew to maturity in a benign (unsafe) environment. The fact that the United States had no reason to exhaust itself to prepare to wage wars against its neighbors separated it from other states, especially the great powers of Europe. America's insular position and existence of loose security fostered the view that war is a derivative of the norms of peace. America's strategic culture was shaped by long periods of peace interrupted by generational conflicts - the War of 1812, the Civil War, World War I, and World War II - defined as a crusade of good against evil. Loose security, on the other hand, affected America's view of the world. As C. Vann Woodward wrote more than four decades ago: "Anxiety for security has kept the growth of optimism within bounds among other people. The relative absence of such anxieties in the past has helped, along with other factors, to create optimism as a national philosophy in America."[4]

---

[3] Colin S. Gray, National Style in Strategy: The American Example, International Security 6, no. 2 (Fall 1981), 22.

[4] C. Vann Woodward, The Age of Reinterpretation, American Historical Review 66 (October 1960), 6.

America's strategic culture clearly rejects the European tradition of political power. This culture clearly enjoys the power of tradition and political power. Rather, since the foundation, Americans have seen themselves as unusual.

Exceptionalism - In the domain of international relations, American exceptionalism refers to the belief that the United States possesses unique qualities or a special destiny that sets it apart from other nations. - influenced the way the United States made deals with others. As Walter Lippmann has proven that America's strategic culture "does not recognize that America is a nation among all other nations that must be dealt with as rivals, as allies, as partners." Moreover, "an aggression is an armed rebellion against the universal and eternal principles of global society. No war can be justly ended, therefore, except by the unlimited subjugation of the aggressors and by the overthrow and transformation of the political regime."[5] The impulse to transform the international system in the service of the ideals of liberal democracy forms a thread that runs through American history. The national security strategy of the Clinton administration and the expansion of the George W. Bush administration's commitment to the spread of democracy exhibiting a long-term impact with unpredictable effects, and after Ukraine the possibility of a conventional attack against the sovereignty and territorial integrity of allies is not excluded.

George Kennan, in his writings on American diplomacy, submitted in 1950, discussed that America's approach to international relations was characterized by excessive "moralism and legalism" leading to a tendency to proclaim crusades against the bad. As Kennan wrote "A war fought in the name of a high moral principle soon finds a form of total domination". Americans have often undertaken wars not as a continuation of policy but as a symptom of their own weakness. JC Wylie was reflecting on a mirrored American view when he wrote: Is war really the continuation of a policy? For us, I believe not. The fight for a non-aggressor nation is in fact almost a complete collapse of politics. Once the war comes, then all pre-war policies become invalid, because the setting in which they were designed to operate no longer corresponds to the facts of reality. When war comes, we immediately move into radically different worlds. Similarly, the United States Army's 1936 text on strategy stated that "Politics and strategy are radically and fundamentally different things.

Strategy begins where politics ends. What the soldiers are asking is that when policy is decided, strategy and command should be considered a separate realm from politics."[6] In other words, Americans tend to think strategically.[7] Thus, the United States has shown a long and consistent preference for starting wars for unlimited

[5] Walter Lippmann, Public Opinion and Foreign Policy in the United States, (London: Allen and Unwin, 1952), 25-26.

[6] The Principles of Strategy for an Independent Corps or Army in a Theater of Operations, (Ft. Leavenworth, KS: Command and General Staff School Press, 1936).

[7] Samuel P. Huntington, The Soldier and the State: The Theory and Practice of Civil-Military Relations, (Cambridge, MA: Belknap Press, 1957), 151.

political reasons.[8] During the Civil War, President Abraham Lincoln, in World War II Franklin D. Roosevelt and his commanders were of one mind that the war should be directed at overthrowing the German, Japanese and Italian governments that had started the war. In the current fight against jihadist extremists there is no feeling that could lead to the establishment of negotiations.[9] Americans have tended to refer to their wars as crusades against evil.

As Samuel Huntington has remarked: "For an American, a war is not a war unless it is a crusade."[10] Undoubtedly, such a viewpoint has strong political roots in the twentieth century. The United States fought a series of despotic regimes, from Hitler's Germany and Kim Sung II's North Korea, to Saddam Hussein's Iraq and Slobodan Milosevic's Serbia. However, there has always been a clear tension between the need to rally the public in support of the use of force and the need to pursue limited goals. Political leaders who demonized America's opponents often faced a backlash when the United States did not continue the war to the end. Advisors to President George. W. Bush, for example, were outraged by the comparisons of Saddam Hussein to Adolf Hitler, fearing that this would bring back the 1991 complicated Gulf War.[11]

Weigley says that for a more critical assessment of the "American Way of War" we need to know: when did the Armed Forces have a unique achievement in combat, in wars where annihilation was done through the excessive use of firepower? In his formulation, the main characteristics of the "American Way of War" include aggressiveness at every level of battle, a concern for decisive wars, and a desire to put up maximum resistance. The United States Army has seen "the complete overthrow of the enemy, the destruction of the military forces, (as) an object of war"[12] Weigley also argues that "Americans, especially American soldiers," have maintained a narrow definition of strategy that tended to "give little consideration to the consequences of non-soldiers in relation to what they were doing." Also, the national strategic, military, and service culture has affected how the United States has approached nuclear weapons. The National Strategic Culture of nuclear weapons has reinforced the old idea in the United States that there is a dichotomy between

[8] As Clausewitz wrote, "War can be of two kinds, in the sense that either the objective is to overthrow the enemy - to render him politically helpless or militarily impotent, thus forcing him to sign whatever peace we please; or merely to occupy some of his frontier districts so that we can annex them or use them for bargaining at the peace negotiations. Transitions from one type to the other will of course recur in my treatment; but the fact that the aims of the two types are quite different must be clear at all times, and their points of irreconcilability brought out [emphasis in original]." Carl von Clausewitz, On War, ed. and trans. Michael Howard and Peter Paret (Princeton: Princeton University Press, 1976), 69

[9] For alternative views, see Eliot A. Cohen, Supreme Command: Soldiers, Statesmen, and Leadership in Wartime (New York: Free Press, 2002), 175-184; Andrew Krepinevich, The Army and Vietnam (Baltimore: Johns Hopkins University Press, 1986).

[10] Samuel P. Huntington, The Soldier and the State: The Theory and Practice of Civil-Military Relations (Cambridge, MA: Belknap Press, 1957), 152.

[11] George Bush and Brent Scowcroft, A World Transformed (New York: Knopf, 1998), 389.

[12] Weigley, American Way of War, xxi

peace and war. Since the beginning of the Cold War, the dominant view maintained by civilian strategists and military officers has been that nuclear weapons are the first and foremost weapons of deterrence. As George Kennan wrote in 1961 that: The atom has simply served to make inevitably clear what it really has been all this time since the day the machine gun and the internal combustion engine were used in the techniques of war.

In its context, the Military Strategy orients the functioning of the defense which can serve until the next decade. As it has been pointed out above by some military thinkers, the Military Strategy is the main planning document of the military instrument of the national power at a strategic level. The security and defense of the country relies on the development and integrated use of elements of national power through a comprehensive inter-institutional approach, oriented by the challenges of the unstable geopolitical environment.

2. The military strategies of some allied states, the case of Romania

Romania is a powerful country committed to European values and plays an important role in NATO and the EU, in guaranteeing the security of their external borders, as well as in the region of the Black Sea. It is also a solid partner for the US and its allies as a pillar of regional security. National security policies cannot be an expression of the will of a single person, although it is the result of a process that falls under the duties of the President. It should be built, at least on principle, on basic values and guidelines, as it is an expression of national consensus and common effort. In relation to the security challenges on the eastern border of NATO and the EU, Romania will establish a stronger anchoring of the two organizations in the region, towards an applied cooperation with regional allies, but also to support the states of the Western Balkans and the eastern neighborhood, in their transformational processes in terms of internal institutions, democracy and connection with European economic flows.

The National Defense Strategy of Romania for the years 2020-2024 provides answers to the main questions regarding the main Romanian national objectives for guaranteeing its security and that of its citizens and outlines the necessary steps to achieve them. In Romania's defense strategy 2020-2024, the measures to be taken against any possible threat are clearly defined, since both Poland and Romania are border countries with the conflict zone in Ukraine.

Over the past 30 years, Romania has evolved significantly thanks to the individual and collective action of its citizens. Romania has fulfilled the national objectives that have been vital for its internal development, as well as for its strengthened position abroad: membership in NATO and the European Union. Regarding Romania's security, in a dynamic, turbulent and unpredictable geopolitical context like the current one, we must have an adapted and efficient response to the risks, threats and vulnerabilities we are facing, based on: continuity, adaptability, flexibility, resilience and predictability. Within NATO, it will continue to act decisively, as in the past, to increase Romania's importance within the Alliance, so that the latter continues to be

the strongest and most efficient collective defense organization in history.

Romania's firm commitment to allocate at least 2% of GDP funding to defense, in addition to the appreciation by allies, has also brought tangible benefits in terms of the country's security. Without strong armed forces, a state does not benefit from international and strategic credibility. The new defense architecture requires highly trained and equipped human resources as well as interoperable capabilities in the NATO collective defense system. The existence of significant resources aimed at providing for the Romanian Armed Forces and guaranteeing their long-term distribution is also a necessary incentive for the revitalization of the national defense industry.

Technological developments generate a diverse and increased complexity of security risks and threats, such as cyber-attacks, information-related activities (hostile/ influential actions carried out in the public space, disinformation, the spread of fake news, etc.), as well as the possible harmful and destabilizing effects caused by introducing some used civilian technologies within asymmetric and hybrid actions, thus bringing new security challenges.

In the social domain, the security environment is affected by asymmetric demographic development, rapid urbanization, polarization of societies, population ageing, increased individualism and isolation in virtual space, increased vulnerability of online social media to information warfare, actions, as well as from the phenomenon of growing migration. At the same time, urbanization is making cities more vulnerable, especially from the perspective of climate change and the provision of minimum standards for living conditions. The National Defense Strategy represents, naturally and legitimately, a synthetic collection of aspirations, desires, visions and ideas of freedom, dignity and prosperity that aim to build a normal Romania: a Romania of the 21st century. The strategy reflects the need to ensure a natural balance between national security and other vital areas such as the economy, health or education.

At the same time, the Strategic Partnership with the USA, especially after the higher level meetings that have taken place over the last few years, has better prospects than ever for deepening and expanding its role as a strategic anchor of the Euro-Atlantic position and its role as a benchmark for other objectives and efforts made to guarantee Romania's national security. The development of the Strategic Partnership with the USA, especially in the economic aspect, with a focus on the domain of latest technologies, will give even more consistency to bilateral relations, and will increase the strategic importance of Romania. Romania intends to strengthen its military cooperation with the USA not only as a line of action aimed generally at the allied format, but especially as an operational objective to be implemented on the national territory. Subsequently, the efforts of the Romanian state are directed towards the implementation of some solutions in Romanian territory aimed at strengthening NATO's advanced presence and, implicitly, preventing possible aggressive actions carried out by some state actors. Military cooperation within the formats established in the region, development and expansion of several broad innovative concepts with allies and European and regional partners, making operational the national initiatives

approved at an allied level, can contribute to the practical implementation of the objective to maintain regional and European security.

Romania's concept of resilience is approached from a dual perspective: the inherent capacity of entities – individuals, communities, regions, the state – to resist and articulately adapt to violent stress-causing events, shocks, disasters, pandemics or conflicts, on the one hand, and the ability of these subjects to return as soon as possible to a functional, normal state, on the other hand. Strengthening resilience and reducing vulnerabilities require a flexible multidimensional strategy, as well as a broad perspective for all systems, in order to limit the risks associated with a crisis, but also to improve the capacity to quickly manage adjustment mechanisms at a local, national and regional level.

In addition to the analysis of the military strategies of some partner states, we must also pay attention to the military strategy or doctrine of our neighbors and mainly that of Serbia. From the published document, Serbia has announced the new military doctrine. *According to the strategy, Serbia's military force should be greater than all the armed forces of potentially adversary countries in the region combined.* From the analysis made and the comparison of the current military power, Serbia reaches the level of 65-70% of the power of the armed forces of Croatia, Bosnia-Herzegovina, Albania and the "unknown state of Kosovo". But according to the analysis this is not enough, therefore it is intended to reach at least 110% of the joint military power of the four mentioned countries. Only if the Serbian army is able to stop the offensive and effectively neutralize the threats of all potentially adversarial countries of the region, can there be a long-term guarantee of peace and stability. Only if these countries know that the military clash with Serbia will cause proportionally greater losses, can Serbia plan its long-term state and social development. In the spirit of this strategy, Serbia has made large investments in the purchase of armaments and in the development of military relations with Russia, even though in that strategy it has proclaimed military neutrality. It is also stated there that the Head of State does not even have the legal authorization to approve a new strategy, because the Parliament of Serbia has that authorization. The head of state can make a proposal to the Parliament for a new strategy or update the existing strategy. Also, the approach to those determinations which are the main pillars where its concrete implementation will take place.

In conclusion, I would like to briefly address something about the draft Security Strategy of the Republic of Kosovo for the year 2022-2027. This project has been approved by the Parliamentary Commission for Security and Defense Affairs, as one of the main challenges for the country's security, which is "Serbia's territorial claim to Kosovo". The risk from Serbia is mentioned for the first time explicitly in such a document. The draft Security Strategy of Kosovo is a document that includes all aspects of the security challenges in Kosovo "...especially the dangers that originate from the neighboring country, Serbia. In this project, the main risk that threatens the state is correctly identified for addressing the identified risks that also include climate change, possible natural and human disasters, violent political

or religious extremism. Also, this draft strategy focuses on "Youth migration as one of the potential risks. But among the elements that are foreseen with risk is the part of preserving the vitality of the security institutions, that they be renewed, in order to ensure a continuity of operation with the recruitment of young people within the Kosovo Security Force, the police, agencies and various services". Likewise, it is stated there that "KSF will constantly review its organizational structure, to adapt to the times and tasks that arise, in order to realize and protect vital state interests".

I think that the project was probably the most advanced of the strategies that were introduced in the early stages by the Government. Based on the analyses and comments, it turns out to be a good strategy project, especially when compared with previous projects or even with the previous National Security Strategy". While it should not be forgotten that the relations with Serbia have not been good since 1998-99, when Serbian regime initiated a war fought in Kosovo, which resulted into over 13,000 dead civilians and thousands of people missing. Over 1,600 people are still missing, most of them Albanians. Serbia does not recognize the independence of Kosovo and in the Constitution continues to consider it as part of its territory. While Kosovo and Serbia have continued talks on the normalization of relations since 2011, with the mediation of the international factor, but the dialogue process has progressed slowly.

Conclusions

- Eastern military strategy differs from that of the West by focusing more on asymmetric warfare and deception. Strategy differs from operations and tactics, as strategy refers to the use of all of a nation's military capabilities through high-level, long-term planning, development, to ensure security or victory.

- Based on the concepts and elements of defense, implementation determinations mainly in strengthening defense against possible attacks, as well as participation in various tasks in the interest of NATO, the EU, the UN, a defined planning should be done clearly, in order for the approved defense budget to be as effective as possible.

- The aggressive behavior of the Russian Federation, actions to militarize the Black Sea region, as well as their hybrid operations carried out in order to maintain a tense climate of insecurity in the vicinity of our region require determination to continue the process of updating the strategic documents of our country.

- As for above, it is important that in the strategic documents of any type of strategy, but especially military one, the essential elements be clearly defined, while these elements should include other supporting documents, such as the Long-Term Plan of Development etc.

References

1. Koncepti i ri Strategjik i Aleancës, Madrid 2022. (The new Strategic Concept of the Alliance, Madrid 2022.)
2. Strategjia Ushtarake e NATO-s e miratuar në 2019. (NATO Military Strategy approved in 2019.)
3. NATO's Concept for Deterrence and Defense of the Euro-Atlantic Area (DDA).
4. The NATO Warfighting Capstone Concept (NWCC).
5. Weigley, American Way of War, xxi
6. The Principles of Strategy for an Independent Corps or Army in a Theater of Operations (Ft. Leavenworth, KS: Command and General Staff School Press, 1936).
7. Samuel P. Huntington, The Soldier and the State: The Theory and Practice of Civil-Military Relations (Cambridge, MA: Belknap Press, 1957), 151
8. Michael Howard and Peter Paret (Princeton: Princeton University Press, 1976), 69.
9. For alternative views, see Eliot A. Cohen, Supreme Command: Soldiers, Statesmen, and Leadership in Wartime (New York: Free Press, 2002), 175-184; Andre Krepinevich, The Army and Vietnam (Baltimore: Johns Hopkins University Press, 1986).
10. Samuel P. Huntington, The Soldier and the State: The Theory and Practice of Civil-Military Relations (Cambridge, MA: Belknap Press, 1957), 152.
11. George Bush and Brent Scowcroft, A World Transformed (New York: Knopf, 1998), 389.
12. C. Vann Woodward, "The Age of Reinterpretation," American Historical Review 66 (October 1960), 6.
13. Walter Lippmann, Public Opinion and Foreign Policy in the United States (London: Allen and Unwin, 1952), 25-26.
14. Colin S. Gray, "National Style in Strategy: The American Example," International Security 6, no. 2 (Fall 1981), 22.
15. Michael I. Handel, "The Evolution of Israeli Strategy: The Psychology of Insecurity and the Quest for Absolute Security" in Williamson Murray, MacGregor Knox, and Alvin Bernstein, eds.
16. The Making of Strategy: Rulers, States, and War (Cambridge: Cambridge University Press, 1994).
17. Michael Evans, The Tyranny of Dissonance: Australia's Strategic Culture and Why of War, 1901-2005 (Canberra: Land Warfare Studies Centre, 2005).

SECOND RUBRIC

ARTIFICIAL INTELLIGENCE AND INNOVATIVE DEVELOPMENTS

National Cyber Security Strategy (NCSS): policy tool to strengthen the cyber security and resilience of CII

Lieutenant Colonel Msc. Dashnor BETA
Military Scientific Research Institute

Abstract

In recent decades, innovation, technological advances, and the widespread use of the Internet have led to profound transformations and challenges in societies worldwide. Information and communication technologies (ICTs) have significantly influenced daily life, human rights, economies, and social interactions. The shared and open nature of cyberspace fosters social and political inclusion, breaks down communication barriers between nations, communities, and individuals, promotes transparency, and enables real-time interaction and the exchange of ideas across the globe. While the growing use of ICTs offers substantial benefits, it also presents significant risks, underscoring the importance of cyber protection and security.

A pressing and increasingly concerning issue for society today is the violation of privacy and identity theft. While governments are investing heavily in digital infrastructure to enhance citizen services, individuals are also turning to the Internet for its numerous advantages. One of the greatest challenges faced by nations is the creation of a developed, cyber-secure digital society, equipped with the knowledge and skills needed to maximize opportunities while effectively minimizing and managing risks. A pivotal component in drafting the legislation and combating cybercrime is the national strategy on cybercrime. National and international structures draft and implement awareness campaigns for various interest groups, with the aim of protecting against cybercrime and other security attacks on the Internet. A legal and regulatory framework that protects against various forms of abuse and electronic crime is essential for creating a trustworthy environment for electronic communications and transactions.

Keywords: National Cyber Security Strategy (NCSS), Critical Infrastructure (CI), Critical Infrastructure Protection (CIP), Critical Information Infrastructure Protection (CIIP), cyber risk, cyberspace, CIP/CIIP regulatory framework, CIIP coordinator

Introduction

Albania, like many other nations, frequently falls victim to malicious cyber activities conducted by criminal actors, including both state and non-state entities, who exploit network infrastructures within the country and beyond. As a developing nation, Albania relies on information and communication technologies (ICTs) to enhance living standards and improve public services. However, alongside the benefits of adopting new digital technologies, the Internet also introduces significant cyber-security challenges. Cyber threats are on the rise, often exploiting technological vulnerabilities or a lack of knowledge in the proper use of digital tools, posing a growing risk to the security of information systems.

At present, there is a lack of essential tools to obtain and create cyber intelligence, to use the necessary human and logistical resources to carry out law enforcement activities. Strengthening capacities to address cyber challenges is crucial and requires structural changes, new approaches, and enhanced technical and logistical capabilities. The advancement of internet infrastructure in our country has facilitated the emergence of cybercrime in various forms, with the most common being internet *banking*, such as *phishing* and *spam*. Even when cybercriminal activities targeting Albania are identified, it is often challenging for law enforcement agencies or international organizations to track down the perpetrators.

Albania has made significant strides in improving cyber-security. In addition to progress in ICT and the digitalization of public services, the legal framework for cyber-security has been enhanced and updated. However, the country has yet to achieve the scale and speed of adaptation required to keep pace with the rapid evolution of various cyber threats. Undeniably, cyber-attacks are among the most critical security challenges of the modern era, making cyber-security a vital component of national security.

1. Review of the NCSS - a necessity to increase the level of cyber-security in the country

In alignment with developed countries, the strategy for ensuring a safer cyber environment should adhere to the following fundamental principles: applying the same core values in both the physical and digital realms; safeguarding fundamental rights, including freedom of expression, personal data, and privacy; universal access; democratic and effective governance; shared responsibility for guaranteeing cyber-security. The motivations for strengthening national cyber-security capabilities may vary from country to country and can include:

a) initiatives by regional organizations (e.g., African Union-AU, Organization of American States-OAS),

b) initiatives by CII provider networks (e.g., Commonwealth Telecommunications Organization),

c) initiatives by international organizations (e.g., the World Bank-WB, the International

Telecommunication Union-ITU, the North Atlantic Treaty Organization-NATO, and the Organization for Economic Co-operation and Development-OECD, which may recommend or pressure countries to pay more attention to national cyber-security issues, including Critical Information Infrastructure Protection (CIIP), such as:

- a reactive measure against systematic cyber-attacks on critical national services;
- preventive measure resulting from a national cyber risk assessment;
- calls from various economic sectors to strengthen national security capabilities and cyber resilience.

In this context, countries initiate discussions at the national level (multi-stakeholder approach), with the support of international partners (e.g., ITU, WB, BA, OAS), to identify gaps, national and sectoral cyber risks, domestic needs, and priorities in the field of cyber-security. The data collected from the public consultation process and various assessments feed into and shape the content of the NCSS. This strategy is essentially a roadmap that defines a set of national strategic objectives to be implemented (and regularly evaluated) within a specific timeframe (fig. 1).

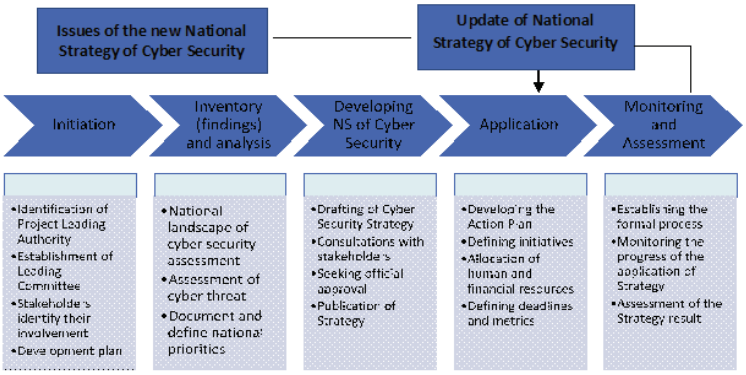


Fig. 1. Life cycle of a National Cyber-security Strategy [1]

First, the NCSS addresses multiple CIIP activities, including identification of national CIs and CIIs, development of the CIIP policy and legal framework, as well as other strategic activities such as: establishing a governing structure and cyber-security coordination program (with defined roles, responsibilities, budget, resources, action plan), setting up a National Computer Security Incident Response Team (CSIRT), adopting a cyber-security action plan and awareness-raising activities, adopting legislative frameworks (e.g., cyber-crime and/or data protection legislation), and adopting domestic and international cooperation mechanisms. A guide to developing an NCSS outlines best practices and CIIP-related activities that the strategy should address to ensure the protection of CI services and essential services such as:

[1] Source: https://ncsguide.org/the-guide/lifecycle/

- adopting a cyber risk management approach (national and sectoral),
- defining a governance model with clearly outlined roles and responsibilities, as well as allocated budgets and resources,
- minimum legislative definition, regulatory bases and technical requirements,
- adopting a wide range of incentives to ensure that CI/CII operators meet minimum technical and legal requirements,
- establishing sustainable and formal public-private partnerships and other informal cooperation agreements.

2. Identification of national CI and CII sectors

Taking into account the above practice and the shared responsibility approach, governments through coordinating authorities are responsible for leading and coordinating the CI/CII identification process.

First step: Identification of CI sectors and services and then of the CII service sectors. We emphasize that not all countries follow this order. Both identification processes require key stakeholders and the active participation of public and private sector CI/CII operators.

The process of identifying CIs can consist of the following steps:

- Adoption of preliminary planning activities to define the scope of the CI identification process, roles, responsibilities and resources.
- Identification of key stakeholders to be involved throughout the CIP/CIIP process, including the national risk assessment and consultations for the identification of CIs. This activity helps to define the governance structure of the CIP and the roles and responsibilities of key IC actors, including coordinating agencies and public and private stakeholders.
- Definition of the risk profile of the country as a whole (national risk assessment) following the different methodologies described below.
- Formal adoption/designation of CI sectors through a CIP policy (e.g., Canada) or legal framework (e.g., Serbia, Montenegro). Once identified, it is recommended that the list of national CI sectors and services be widely distributed.

As part of the CI identification process, some countries adopt policies/legal frameworks that define the identification methodology and other security requirements (e.g., Montenegro), while other countries implement risk assessment methods provided by international partners. Countries also appoint a coordinating body to lead the process of identifying CIs/CIIs and further CIP activities.

As the cyber threat landscape changes rapidly, it is recommended that coordinating authorities annually conduct national cyber risk assessments to identify new risks and, therefore, new critical services or assets.

Second step: Identification of CII sectors and services. Similar steps, processes and methodologies can be followed for this; however, the identification of CII is often more complex than that of CI.

Third step: Identification of CII subsectors and services, within those CI/CII sectors and specific CII assets that support CI services (fig. 2).

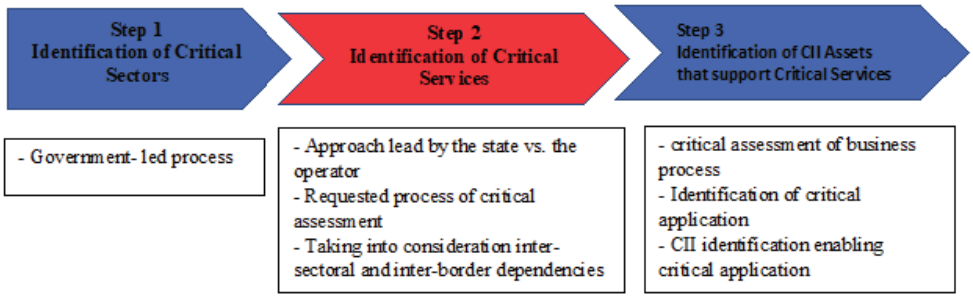


Fig. 2. CII identification steps (ENISA - 2014)

The EU has approved Directive 2008/114/EC, which defines the procedure for the identification and designation of Critical European Infrastructures (CEI) in the transport and energy sectors that had significant cross-border impacts. It provides a common approach by assessing the need to improve the protection of certain CIIs. Montenegro has adopted a law on the designation and protection of CI in 2020 to establish the criteria and requirements for the identification of CII according to the standards of the NIS (Network and Information Security) Directive.

Key CI/CII stakeholders

Identifying key CI/CII stakeholders who should be involved throughout the CIP/CIIP process is vital. There is no exhaustive list of CI/CII stakeholders, as different countries may adopt different approaches. Some countries have included public and private sector organizations (e.g., CI/CII operators), academia, civil society groups, technical bodies, law enforcement agencies, international partners, etc. (list 1 below).

List 1: (non-exhaustive) list of CI and CII stakeholders.

- ✓ CIIP coordinating agencies: of Interior, of Justice, ICT; of Defence, Prime Minister's office.
- ✓ ICT Ministries: Communication, Media, ICT departments.
- ✓ Ministries responsible for specific CI: Department of Economy, Energy, Health.
- ✓ Regulators for specific CI areas: ICT, Financial, and Energy Regulator.
- ✓ Law enforcement agencies and similar.
- ✓ National security and intelligence agencies.
- ✓ Crisis management and security agencies.
- ✓ Public and private CI and CII operators (and owners) of the respective companies.

- ✓ Politicians and parties.
- ✓ ICT security companies, software vendors, SCADA (**S**upervisory **C**ontrol and **D**ata **A**cquisition - a control system architecture that includes computers, networked data communications, and graphical user interfaces for high-level machine and process supervision) manufacturers, system integrators and third-party maintenance companies.
- ✓ Intersectoral organizations.
- ✓ National and sectoral CSIRT teams.
- ✓ National Cyber Security Centers.
- ✓ Academics, researchers and developers.

3. National cyber risk assessment

Effective risk assessment methodologies are the foundation of a successful national CIP and CIIP program. Adopting a risk management approach is necessary to identify current threats, assess vulnerabilities and their impact on CI and CII assets, systems or networks, taking into account the probability of occurrence of these threats.

The guide for the development of NCSS and the GFCE-Meridian report on the CIIP recommend conducting national/sectoral risk profiles to identify the risk of failure of CI and CII sectors/services. The purpose of these profiles is to establish a shared understanding of the risk factors affecting a specific country/sector of the economy, through a systematic assessment of the threats and consequences of CI and CII failure. Systematic threat assessment means that all threats are evaluated based on their impact and likelihood of occurrence. The outcome of this risk assessment provides an overview of the risk factors and their position in relation to the impact and frequency of occurrence. Each risk that is addressed as a national/sectoral risk profile can form the basis of an integrated national/sectoral approach to its prevention, preparedness and response. Considering the risks associated with CIs and CIIs in the context of a national / sectoral risk profile can help develop an integrated and balanced risk management approach that supports CIP and CIIP.

Areas of risk assessment:

a. Organizational approach of ICT systems (e.g., the US National Institute of Standards and Technology's Framework for Improving IC Cybersecurity and the United Kingdom (UK) Technical Risk Assessment Standard No. 1);

b. Sectoral level approach (e.g., infrastructure risk and resilience methodology).

c. National level approach (e.g., the 2020 national cyber threat assessment - Canada, and the national cyber risk assessment implemented by the UK Foreign and Commonwealth Office and in many Commonwealth countries in Africa and the Caribbean).

d. Regional level approach (e.g., EU Risk Management Capability Assessment

Guidelines (RMCA), which support national authorities in determining the national risk profile. RMCA is a non-binding, comprehensive and flexible methodology, enabling national authorities to self-assess their risk management capability).

According to the EU Agency for Cyber Security (The European Union Agency for Cybersecurity - ENISA) there are two basic approaches to risk assessment at the national level:

a. Centralized assessment/state-led approach: This is a one-size-fits-all model; the coordinating authority requires that the identified actors (CI operators) apply a separate or unified standard for risk assessments. This type of approach has been implemented by the UK.

b. Decentralized evaluation/operator-driven approach: In this approach, each identified actor (CI operator) prepares its own risk assessment to be integrated by a coordinating authority. This approach has been implemented by the Nordic countries, Sweden, Denmark, Japan, Switzerland.

In addition to the above, different methodologies/approaches can also be used, such as:

- ***Scenario-based approach:*** According to this, the identified actors gather to review the scenarios in a circular fashion; such scenarios describe risks as a narrative and label them by applying simple categories of likelihood and impact (low, medium, high). This risk assessment approach is used by the telecommunications sector in Denmark.
- ***Quality approach:*** Countries with a specific threat modeling technique tend to use qualitative models. Qualitative assessments are the common approach used by countries when deciding on the significance of a threat. This model, where there is a wide range of threats, is common in the Nordic countries.
- ***Quantitative approach:*** This approach applies ordinal thresholds (e.g., specific risks are classified as severe if they affect 200 in 20,000 or service disruptions for five days or more). Japan is one of the countries that has implemented this approach.
- ***Hybrid approach:*** combines all the above elements (using scenarios and then qualitative and quantitative methods). The Netherlands is one of the countries that has implemented this model.

4. CIIP policy and legal frameworks

The foundations of the CII/CIIP policy and legal framework are:

- Government leadership and engagement, which establishes effective coordination between the government and the public and private CI/CII operators,

- Shared responsibility approach, where the government, the public and the private CI/CII operators are jointly responsible for the protection of CI/CII sectors/assets. So, the government is responsible for ensuring the security and the continuity of

critical sectors and services, while CI/CII operators are responsible for the security of their infrastructure needed to provide the critical service. Each state must, at a minimum, develop and adopt a basic CIIP regulatory framework that includes the following activities:

a) identification and regular reassessment of sectors and services of CII;

b) appointing a coordinating agency with clear legal mandate, roles and responsibilities and sufficient resources to act as such;

c) security requirements and legal obligations, such as regular risk management assessments, audit mechanisms, vulnerability disclosure mechanisms, information sharing, incident reporting obligations, CI/CII supply chain security requirements;

d) sustainable public-private partnerships;

e) cooperation mechanisms with regulatory bodies, government agencies, international partners;

f) public awareness campaign.

If there are no CSIRTs, coordinating authorities should consider establishing a national CSIRT with clear instructions to support CI and CII, or seek technical support from other domestic incident response teams (e.g., military/defence CSIRT), until the creation of the national CSIRT.

Models of CIIP regulatory frameworks

Usually, countries change their CIIP regulatory stance to keep pace with the rapidly changing environment. So, the US first adopted the "hands off" approach and then chose a self-regulatory approach. Coordinating authorities can consider a wide range of policy and legal options to ensure that domestic CII sectors and services are adequately protected. The adoption of any policy and legal option depends on factors such as; internal needs and priorities, the level of cybersecurity maturity of the country in general and the ecosystem of CIs/CIIs, the type of threats they face, the type of stakeholders involved in the CIIP, and the government stance.

Government intervention and ***regulatory continuity*** are the two main components that define CIIP regulatory framework options. From a theoretical perspective, the GFCE-Meridian report on CIIP, as well as other research organizations suggest that CIIP regulatory framework choices include: (fig. 3)

✓ Market mechanisms and incentives (known as the "hands-off" approach).

✓ Self-regulation, which includes two subcategories: voluntary and mandatory self-regulation.

✓ The legal and regulatory framework, which includes two subcategories: command-and-control regulation and the government's mandatory program.

✓ Government ownership.

✓ Government ownership.

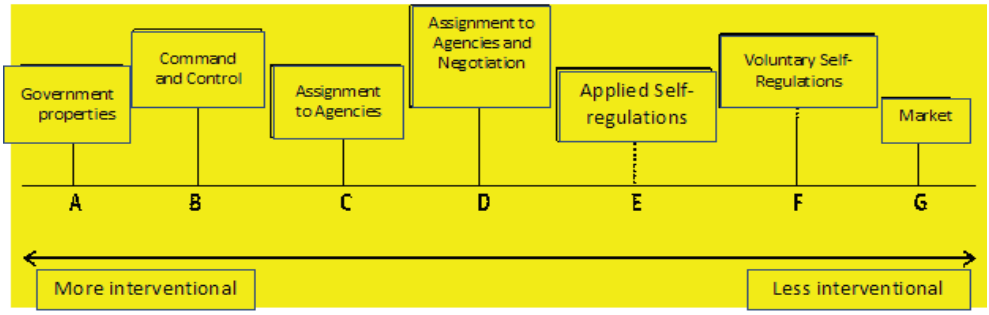


Fig. 3. Models of CIIP regulatory frameworks.

CIP/CIIP governance and regulatory frameworks.

Examples of these frameworks are presented in the following tables:

Table 1. *Governance and regulatory frameworks of CIP/CIIP in the European Union (EU)*[2]

Definition of CI/CII	"Essential Services" refers to "Essential Services of Operators" - public or private entities including energy, transport, banks, financial market infrastructure, health, drinking water supply and distribution and digital infrastructure sectors and those that meet the criteria defined in Article 5 (2).
Governing authority	The EU Cyber Security Agency (ENISA) can support and facilitate strategic cooperation between EU member states regarding information security systems and compliance with other functions defined in the NIS directive.
Regulatory approach **Governing structure**	The NIS Directive was the first mandatory piece of EU cyber security. The directive should become part of the internal legislation of each member state. The EU Cyber Security Agency is the lead authority. Each member country is required to create strategic directives and NIS regulations, one or more CSIRTs, designation of competent authority and contact point.
Critical Sectors	Energy, transport, banking, financial market infrastructure, health, drinking water support and distribution and digital infrastructure.
Appropriate policies and rules	- EU Cyber Security Strategy. - EU Network and Information Security Directive - 08 August 2016. - Cyber Security Act, 2019.

[2] Source:https://ec.europa.eu/jrc/en/research-topic/critical-infrastructure-protection.

Table 2. *Governance and regulatory frameworks of CIP/CIIP in Serbia*[3]

Definition of CI/CII	ICT systems of particular importance are systems used for; (i) Performing duties in public authorities. (ii) Processing of special categories of personal data according to the meaning of the law that regulates the protection of personal data. (iii) Carrying out activities of general interest and economic activities in the fields of: (a) energy, (b) transport, (c) health sector, (d) banking and financial market, (e) digital infrastructure, (f) public goods, (g) social information service, (h) other fields... (iv) Legal entities and institutions established in Serbia and local self-government units for the performance of the activities detailed in section (iii) above.
Governing authority	Ministry of Interior (MoI) (competent authorities) and the Ministry of Trade, Tourism and Telecommunications (competent authorities for cyber security).
Regulatory approach **Governing Structure**	Existing legal and regulatory frameworks are binding on CIs and CII operators. Ministry of Interior coordinates and supervises the operators of CIs, while the operators of ICT systems of special importance are supervised by the Ministry of Trade, Tourism and Telecommunications.
Critical Sectors	Critical national sectors: energy, traffic, food and water support, health care, telecommunications and telecommunications technology, environmental protection, functioning of government entities.
Appropriate policies and rules	- Information Security Law (2016) - Critical Infrastructure Law (2018) - Information Development Strategy - Security Strategy 2017-2020.

[3] Source: Interview with Natalija Radoja, February 19, 2021.

Table 3. *CIP/CIIP governance and regulatory frameworks in the US*[4]

Definition of CI/CII	"... systems and assets, physical or virtual, so vital to the US that their incapacitation/destruction could have debilitating impacts on security, national economic security, national public health security, or some combination thereof".
Governing authority	The Cyber-security and Infrastructure Security Agency (CISA) is part of the Department of National Defense and coordinates efforts to strengthen security using trusted partners across the public and private sectors and provides technical assistance and conducts assessments of federal actors, as well as infrastructure owners and operators across the country.
Regulatory approach	National Institute of Standards and Technology issues the Framework for Improving CI Cyber-security. The Framework is a set of voluntary, risk-based standards and best practices to help organizations of all sizes manage cyber security in any sector. Sector-specific agencies have adopted a multifaceted approach that includes cyber security activities; mandatory and voluntary ones.
Governing Structure	The Department of National Defense is responsible for 10 of the 16 identified sectors. The Departments of Energy, Defense, Treasury, Agriculture, Health and Human Services, General Services Administration, and Environmental Protection are responsible for other sectors. The Infrastructure Protection Office, including the Infrastructure Protection and Cyber Security Agency, is responsible for coordinating the protection of CI at the national level.
Critical Sectors	Chemical, commercial facilities, communications, critical manufacturing, dams, defense industry bases, emergency services, energy, financial services, food and agriculture, government buildings, healthcare and public health, ICT, nuclear reactors, materials and waste, transport, water and sewage. In 2020, the US also identified the core workforce of CIs.
Appropriate policies and rules	- Presidential Policy Directive 21 (Security and Resilience of CIs). - Strengthening Cybersecurity Act of 2014. - National Cyber Security Protection Advancement Act of 2015. - Cybersecurity Information Sharing Act of 2015. - Cyber Security and Infrastructure Security Agency Act 2018. - Framework for Improving CI Cyber Security.

[4] Source: Interview with Paul Rosenzweig, February 25, 2021.

CIIP National / Sectoral Coordinators.

The International Telecommunication Information Technology Union's regulatory database shows that 89 of the world's 195 countries have adopted CIIP programs and related regulatory frameworks. In 51 countries, the ICT regulator is responsible for CIIP, mainly in Africa and Europe, where ICT regulators have an active role in protecting CII[5]. These statistics also show that 38 countries have CIIP programs and regulatory frameworks; however, the national coordinating role of CIIP is played by other government agencies. Also, 106 out of 195 countries have no CIIP program or regulatory framework, which is still significant considering the current cyber threat landscape and the importance of protecting CIIP sectors and services.

The statistics above show that there are at least two main profiles of CIIP coordinators:

a) ***ICT regulators,*** and

b) ***Other government agencies*** (e.g., an independent government agency or a government ministry).

Although countries may adopt different approaches in this regard, national or sectoral coordination of the CIIP may be within the mandate of the following entities:

a) ***The ICT regulator*** The Communications Regulatory Authority (Malawi) and the Telecommunications Regulatory Authority (United Arab Emirates), are the CIIP coordinator at the national level. The Finnish Communications Regulatory Authority and the Swedish Post and Telecom Authority are the main government agencies responsible for CIIP – (CIIP coordinator at sector level).

b) ***An independent government agency, center or committee***, the National Center for the Protection of CI in Spain (CIP/CIIP), the Cyber Security and Infrastructure Security Agency in the US (CIP/CIIP), the Information Security Agency in Estonia, and the National Agency for Systems Security of Information (CIIP) in France.

c) ***One of the government ministries***: Ministry of Internal Affairs or Ministry of ICT. In Serbia, the Ministry of Interior deals with CIP, while the Ministry of ICT is responsible for CIIP.

d) ***A computer security incident response team***, - in Latvia this institution is responsible for the daily routine operation of CIIP.

In some countries, the national CIIP coordination role is played by one or more government authorities. For example, in the Czech Republic the national CSIRT and the National Security Agency have joint responsibility for the protection of CIIP service sectors. In France, the French National Cyber Security Agency (ANSSI) is the main government agency dealing with CIIP. At the ministerial level, the Ministry of Interior (e.g., Germany, Hungary) or the Ministry of Defense (Denmark, Latvia) are usually involved in CIIP activities. Mostly this happens in European and African countries.

[5] Source: ITU World Telecommunication/ICT Regulatory Database.

Where there is a defined CIIP policy and regulatory framework, the national CIIP coordinator will have specific legal mandates, functions and responsibilities to interact with the CII community. This legal mandate can be broad-national level (Malawi), or limited-sectoral level (Finland) and must have sufficient technological, financial and human resources to operate as such. The CIIP national coordinator must ensure that CII operators comply with CIIP policies and regulatory framework, including security requirements and legal obligations as minimum standards. This coordinator should also develop and promote local and international cooperation agreements between key CII actors and international partners. Currently, most countries do not yet have a CIIP regulatory framework in place. Fig. 4 shows countries with NCSS that address CIIP and resilience plans (plans of regenerative capabilities).

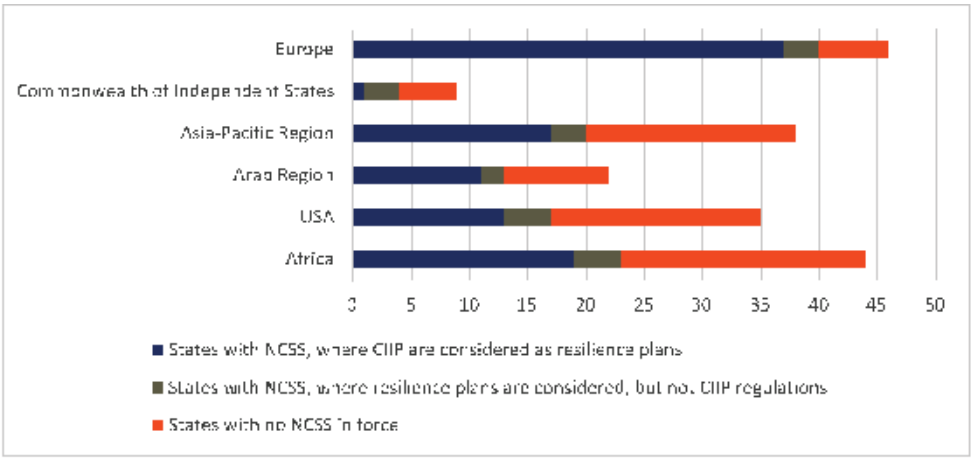


Fig. 4. Countries with an NCSS that address CIIP and cyber resilience plans[6].

In this context, should sectoral regulators, including ICT regulators, adopt a proactive cyber security stance to ensure that CI/CII sectors and services are adequately protected? If competent authorities, including ICT regulators, do not take any action, national CII sectors and services are not safe; and therefore, CII and CI sectors are highly exposed to the risks of cyber vulnerabilities.

In these countries, it is recommended that at least ICT regulators adopt a proactive cyber security stance and find the appropriate legal way to compel CII operators to meet some basic security requirements (e.g., regular cyber risk assessments and internationally recognized standards) and legal obligations (e.g., incident reporting) to ensure that CII is secure. ICT regulators typically do not have the resources and capacity to provide technical support (e.g., incident response management) when cyber incidents occur, unless there is a sectoral CSIRT (e.g., COMM-CSIRT Botswana[7], NCSC-FI in Finland.

[6] Source: ITU 2021.

[7] BW-CIRT.https://www.bocra.org.bw/bw-cirt

ICT regulators should consider establishing formal communication channels to exchange information with ICT operators and other relevant actors in times of crisis. Likewise, ICT regulators should consider establishing communication and cooperation mechanisms with national, local or sectoral CSIRTs, law enforcement agencies and international partners. As CII operators are usually diligent, especially multinational companies, their minimum security requirements and legal obligations will help CII operators detect and mitigate the negative impact of cyber incidents. At the same time, the competent authorities should develop CIIP programs, establish governance structures, as well as draft policies and legal frameworks.

Conclusions

Cyber-attacks are among the most important security threats to the modern world and therefore cyber security has become an important part of national security.

The NCSS is essentially the roadmap that sets out a set of national strategic objectives to be implemented (and regularly assessed) within a specific time frame.

The NCSS is considered an important step in the development of legislation and measures against cybercrime and it should be based on some essential principles discussed above.

Due to the lack of necessary tools, human and logistical resources to exercise law enforcement activity, the increase of capabilities for facing cyber challenges is essential and structural changes, approaches, technical and logistical capabilities are required.

Despite advancements in ICT and the digitalization of public services, along with improvements in the legal framework for cybersecurity in our country, the scale and speed of progress remain insufficient to keep pace with the rapid evolution and increasing complexity of cyber threats.

Different countries adopt a different approach regarding the CI/CII stakeholder list which includes public and private sector organizations, academia, civil society groups, technical bodies, law enforcement agencies, international partners etc.

References:

1. Assaf, Dan, “Models of Critical Information Infrastructure Protection.” International Journal of Critical Infrastructure Protection 1: 6-14, 2008. : Source: https://www.academia.edu/2114887/Models_of_critical_information_infrastructure_protection.
2. Boyens, Jon, and others. 2021. NIST. Key Practices in Cyber Supply Chain Risk Management: Observations from Industry. NISTIR 8276. Source: https://doi.org/10.6028/NIST.IR.8276.

3. Brunner, Elgin M., and Manuel Suter. 2008. International CIIP Handbook 2008/2009. Center for Security Studies, ETH Zurich. Source: https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CIIP-HB-08-09.pdf.

4. Burnett, Peter. 2016. The Critical Importance of CIIP to Cybersecurity. Source: https://www.itu.int/en/ITU-D/Regional Presence/Europe/Documents/Events/2016/Cybersecurity%20Forum%20Bulgaria/GFCE-MERIDIAN%20CIIPv2%20REV. pdf.

5. CSA (Cyber Security Agency of Singapore). 2019. Guide to Conducting Cybersecurity Risk Assessment for Critical Information Infrastructure. Source: https://www.csa.gov.sg/-/media/csa/documents/legislation_supplementary_references/guide_to_conducting_cybersecurity_risk_assessment_for_cii.pdf

6. DCMS (Department for Digital, Culture Media and Sport). 2018. Security of Network and Information Systems. Source: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/677065/NIS_Consultation_Response_-_Government_Policy_Response.pdf

7. Duane, Verner, Frederic Petit, and Kibaek Kim. 2017. "Incorporating Prioritization in Critical Infrastructure Security and Resilience Programs." Homeland Security Affairs 13, Article 7. Source: https://www.hsaj.org/articles/14091

8. ENISA (European Agency for Cybersecurity). n.d. Baseline Capabilities of National Governmental CERTs. Part 2: Policy Recommendations. Source:

9. https://www.enisa.europa.eu/publications/baseline-capabilities-of-national-governmental-certs-policy recommendations/at_download/fullReport#:~:text=Therefore%20a%20national%20%2F%20governmental%20CERT,the%20public%20and%20private%20sectors.

10. ENISA (European Agency for Cybersecurity). 2014. Methodologies for the Identification of Critical Information Infrastructure Assets and Services. Source: https://www.enisa.europa.eu/publications/methodologies-for-the-identification-of-ciis/at_download/fullReport.

11. ENISA (European Agency for Cybersecurity). 2019. Study on CSIRT Landscape and IR capabilities in Europe 2025. Source: https://www.enisa.europa.eu/publications/study-on-csirt-landscape-and-ir-capabilities-in-europe-2025.

12. Garcia Zaballos, Antonio and Inkyung Jeun. 2016. Best Practices for Critical Information Infrastructure Protection. Experiences for Latin America and the Caribbean and Selected Countries. Inter-American Development Bank. Source: https://publications.iadb.org/publications/english/document/Best-Practices-for-Critical-Information-Infrastructure-Protection-(CIIP)-Experiences-from-Latin-America-and-the-Caribbean-and-Selected-Countries.pdf.

13. Giannopoulos, Georgios, Roberto Filippini, and Muriel Schimmer. 2012. Risk

Assessment Methodologies for Critical Infrastructure Protection. Part I: A State of the Art. Ispra: European Commission, Joint Research Centre, Institute for the Protection and Security of the Citizen. Source: https://publications.jrc.ec.europa.eu/repository/bitstream/JRC70046/lbna25286enn.pdf.

14. INSA (Intelligence and National Security Alliance). 2018. Managing a Cyber Attack on Critical Infrastructure: Challenges of Federal, State, Local and Private Sector Collaboration. Source: https://www.insaonline.org/wp-content/uploads/2018/08/INSA-Managing-Cyber-Attack-Critical-Infrastructure.pdf.
15. INTERPOL. 2020. COVID-19 Cybercrime Analysis Report. Source: https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19.
16. ITU (International Telecommunication Union). 2021. Global Cybersecurity Index v4. Geneva: ITU. https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx.
17. ITU, World Bank and partners. 2021. Guide to Developing a National Cybersecurity Strategy. https://ncsguide.org/the-guide/lifecycle/

Artificial Intelligence Developments in the US, EU and NATO Countries and their Impact on Defense and Global Security

Colonel (R) Msc. Dilaver HOXHA

Deputy Director of the Military Scientific Research Institute

Abstract

The Artificial Intelligence (AI) industry is rapidly advancing across various critical areas of human activity. Among the early pioneers in this industry was DeepMind, a subsidiary of Google's parent company, followed by substantial investments from major technology giants like Microsoft, Alphabet, Amazon, Meta, and Apple. "However, ChatGPT, an advanced chatbot-style AI developed by OpenAI, has had the most notable global impact so far, allowing users to pose complex questions and receive responses based on its expansive, publicly accessible data..."[1]. AI, as a branch of computing, is dedicated to developing systems that perform tasks traditionally reliant on human intelligence, including learning, problem-solving, decision-making, perception, creativity, and social interaction. This industry is further bolstered by the contributions of numerous other powerful technology companies, which apply AI across diverse fields such as: education, meteorology, agriculture, transportation, defense, security, and space exploration.

This paper aims to provide an overview of the potential applications of AI in the US, EU countries, and NATO's strategy in this direction, with a focus on its impact in the field of defense. Broadly, AI is a scientific discipline closely linked to numerous other fields and is poised to be a major strategic influence globally in the coming decades. This paper will explore AI trends, key areas of development, and evaluate both the advantages and challenges, especially in simulation systems, defense planning, the military industry, and military operations development.

Keywords: artificial intelligence (AI), machine learning, deep learning (DL), computer vision (CV).

[1] QinetiQ: Will Artificial Intelligence command the army of the future?. 19.10.2023.

Introduction

Technological developments, shaped by both enabling and limiting factors, are driven from human ambition to fulfill the demands and needs for the modernization of essential activities. In various eras, various fields have advanced in response to these needs, with recent decades seeing significant developments in computing - particularly in Artificial Intelligence**.** From the mid-1900s onwards, the field of AI has experienced phases of rapid growth alongside numerous challenges and issues that have been central to efforts aimed at their resolution. In 1956, John McCarthy introduced the term "artificial intelligence", defining it as the science and engineering of creating intelligent machines[2]. Over the past twenty years, AI research, development, and applications have surged, steadily integrating into the global economy through sectors like manufacturing and consumer services[3].

1. Artificial intelligence and its evolution

The rapid global advancement of Artificial Intelligence (AI) has made it one of today's most significant topics. Once a subject confined to philosophy and science fiction, AI is now a reality, widely recognized and heavily invested in by leading companies worldwide. While there is still no universally accepted definition of AI, it is best understood not as a single application but as a transformative technology that enhances and supports a wide range of existing functional applications.

Generally, Artificial Intelligence (AI) relies on data to address specific problems and can be defined as follows*:* "AI is a branch of computer science that combines theory with the development of computer systems capable of performing tasks that require human-like intelligence. These functions include visual perception, speech recognition, language pattern analysis, decision-making, and judgment, emulating the capabilities of human cognition.*"*

In practical terms, Artificial Intelligence (AI) refers to the simulation of human intelligence by machines, particularly computer systems, to perform tasks involving the acquisition, storage, adaptation, transfer, and modification of data. Simply put, AI is computer technology designed to mimic human thinking processes, enabling machines not only to "think" like humans but also to perform tasks even more "intelligently". Specific applications of AI encompass expert systems, natural language processing, speech recognition, and machine vision [4]. AI programming targets key cognitive abilities: (1) Learning – obtaining data and processing data to derive actionable insights); (2) Reasoning - selecting the optimal algorithm to attain

[2] Toneo.ai.

[3] 2019 Annual Presidential Report of the NATO Parliamentary Assembly released 23 mars 2020.

[4] By Nicole Laskowski: according to news director, industry editor, Linda Tucci -- CIO/IT Strategy.

the intended outcomes; (3) Self-correction - refining algorithms continuously[5] to ensure they deliver the most accurate possible outcomes; (4) Creativity - leveraging memory networks, rule-based systems, statistical methods, and other techniques to generate and evaluate new ideas, images, and outputs.

2. Other key definitions related to AI[6]

AI cannot function in isolation; it is interconnected with, dependent on, or interactive with several other fields. Some of these include:

Artificial General Intelligence (AGI): Refers to future AI systems that have the potential to match, and eventually surpass, human cognitive abilities across all tasks of economic significance.

Generative AI: A category of AI systems that can create new content—such as text, images, audio, or 3D assets—based on given prompts or requests.

Large Language Model (Large Language Model- LM): AI models trained on vast amounts of textual data, enabling them to generate human-like responses or predict speech in a self-supervised way.

Natural Language Processing (Natural Language Processing -NLP): The ability of AI programs to comprehend human language, whether spoken or written.

AI Agent: Software systems designed to autonomously perceive their environment, make decisions, and take actions to achieve specific objectives, often without human input. These agents learn from their surroundings and experiences.

Computer Vision (Computer Vision - CV): The ability of AI programs to interpret and analyze images and videos.

Machine Learning (Machine Learning-ML): A branch of AI focused on enabling computers to learn and perform like humans.

Deep Learning (Deep Learning-DL): A subset of machine learning that imitates the human brain's structure, capable of processing, interpreting and handling data sets in order to perform tasks far more complex than humans.

According to the degree of their impact, AI can be classified into the following three categories:

Weak AI: This refers to a computer system that is designed to perform specific tasks more efficiently than humans. This system has been implemented across a wide range of applications.

Strong AI: This refers to systems that can surpass human achievements in any

[5] Algorithm: A process or set of rules to be followed in problem-solving calculations, especially by a computer.

[6] Definitions sourced from the 2023 State of AI report, ChatGTP France, Entreprisedna.co, Futura-Sciences.com.

intellectual task. Examples include robots like demining robots, which operate according to their goals, based on conscious reasoning.

Super AI (SAI): This is expected to surpass human intelligence across nearly all fields, including scientific creativity, logic, wisdom, and social skills. However, scientists argue that human involvement in AI application remains crucial at certain stages, as motivations, ethical considerations, intuition, and particularly spiritual attributes are inherent to humans, even though machines may be capable of imitating some of these traits to a certain extent.

Some of the companies in EU countries that are developing AI are:

The EU and its member states have placed significant focus on AI, as evidenced by the funding allocated to startups specializing in this high-demand technology, which was more than $1.8 miliard by 2023. Many of Europe's leading companies are at the forefront of AI exploration and application, with developments that often surpass the global average. According to available data, while the EU does not have direct competence in military AI, it possesses a range of tools that can indirectly influence the sector, with the defense industry being one such tool. Some of the European AI companies that are seeking market areas and funding sources to compete on a global scale include Mistral AI, Aleph Alpha AI, Owkin AI, and Helsing AI, among others. Notably, only one of these companies, Helsing AI, has applied AI in the field of defense.

However, to achieve further growth, European technology companies planning to implement AI in the military field, need not only sufficient funding but also a robust infrastructure, particularly for data collection and processing centers.

3. NATO Strategy on Artificial Intelligence

AI is changing the global defense and security environment, offering an unprecedented opportunity to strengthen the technological edge of NATO's countries to meet current and future threats in fulfilling the Alliance's core tasks: collective defense, crisis management, and cooperative security. In this regard, NATO and its member countries are committed to cooperation on all matters related to AI for transatlantic defense and security, as set out in the NATO's Strategy on AI.

In its policies and strategy, NATO guides and encourages the development and use of AI in a responsible manner for the defense and security purposes of Allies. The use cases of AI, the creation of new structures and programs for its functioning, will increase interoperability within the Alliance, in terms of protection and monitoring of AI technology. NATO also aims to increase the capacities to renew it periodically, addressing security policy considerations for effective operationalization and protection against potential threats. Keeping pace with AI development is oriented through cooperation between Alliance structures, its member and partner countries, the private sector, and scientific institutions. NATO has defined in its policies the provision of AI talent expertise, the construction of a strong and secure infrastructure,

and the appropriate cyber defenses. Building on NATO's innovation policies, its members' national AI testing centres can support the ambition to develop this science. NATO and its Allies are engaged with powerful technology companies to help shape the development of technologies in the field of AI, creating a shared understanding of the opportunities and risks arising from AI.

At the heart of this strategy are NATO's principles for the use of AI in defense, aligned with international values, norms, and law. These principles are grounded in existing and widely accepted commitments by Alliance countries. NATO's fundamental principles for the use of AI in defense include: legality, responsibility and accountability, explanation and traceability, reliability, direction, and mitigation of bias[7].

NATO is working to define international AI standards to ensure full coherence throughout the entire lifecycle of its operation. Special attention is being paid to the private sector, which includes Big Tech companies, new businesses, entrepreneurs, and experts in the AI field.

4. The most useful current military applications of AI in the US

There is a clear global trend toward adopting AI-driven technologies in military applications, with countries like the United States, China, and Russia leading the way in integrating AI into defense operations. These nations are making substantial investments in AI research and development, particularly focused on creating autonomous systems, predictive analytics, and intelligent decision-support tools to enhance the efficiency and effectiveness of military capabilities.

The U.S. military has been utilizing AI for many years, even before its widespread adoption in civilian life. Over time, these AI systems have evolved to handle complex and multifaceted tasks, minimizing the need for human intervention-though always under human supervision. Currently, AI has achieved remarkable progress in enhancing the operational capabilities of the U.S. military and supporting the successful execution of its military missions.

In November 2023, the U.S. Department of Defense released a strategy for adopting advanced AI capabilities to maintain decision-making superiority on the battlefield. This strategy has influenced the development of AI, and reinforced the U.S. competitive edge in global technological advancements. "While our focus has been on responsibly and swiftly integrating AI into our operations, our primary motivation is straightforward, as it enhances our decision-making advantage..... As commercial technology companies and others continue to expand AI's boundaries, we are committed to staying ahead with foregisht, responsibility, and a deep understanding of the broader implications for our nation." [8]

[7] North Atlantic Treaty Organization, First-Ever Strategy for Artificial Intelligence, released 22 October 2021.

[8] Deputy Secretary of Defense Kathleen Hicks, during the strategy release ceremony at the Pentagon, 2 November 2023.

Similarly, the Head of State Department for Digital Defense and AI, Craig Martell has stressed “Technologies evolve, and things will change next week, next year, and next decade. What succeeds today may not succeed tomorrow...”.

AI is being deployed across various areas of military activity, including data collection, processing, and analysis; development of simulations and combat scenarios; operational planning, decision-making, and implementation monitoring; logistical and medical support; system maintenance and troop transportation; as well as personnel training and educational programs. For AI systems to be effective, however, they must be implemented according to best practices and in the most suitable ways.

Some of the main areas where AI technology is being used in the U.S. military are:

Autonomous Weapon Systems: These AI-powered systems can independently identify, track and engage targets with minimal human involvement, reducing the risk of human and material losses while enhancing the effectiveness of military operations. Examples include autonomous weapons, sensors, navigation systems, aviation support, and surveillance technologies. The primary goal of these systems is to increase operational efficiency and reduce reliance on human input.

Strategic decision-making: This approach combines human ethical judgment with the rapid analytical capabilities of AI, accelerating the decision-making process. AI can swiftly collect, process, and analyze data from multiple sources with high accuracy, assisting leaders in planning and making informed decisions, particularly in critical situations. Additionally, AI can generate simulations to test potential scenarios, supporting more precise decisions - always under close human supervision.

Unmanned Aerial Vehicles (UAVs): AI technology has become integral to UAVs, significantly transforming their efficiency. In earlier models, human operators made essential decisions, but advancements in AI now allow the latest generation of UAVs to operate autonomously with minimal intervention. AI has also improved the coordination of UAV groups, or “drone swarms,” which can be deployed in both simulations and live training exercises.

Data Mining and Processing: This is useful for quickly filtering data, selecting the most valuable information, elimininating redundancies, and reducing human error. This enables military personnel to identify patterns more efficiently, draw accurate conclusions, and develop action plans with a more comprehensive view of the situation. Based on these developments, military leaders can craft strategies based on a thorough understanding of current conditions and predictions for the future.

Threat prediction, monitoring, and situational awarness: This process involves operations that collect and analyze information to support various military activities. Regarding the monitoring of threats, there are unmanned systems (such as drones) that can either be remotely controlled or sent along a predetermined route. These systems leverage AI to assist personnel in monitoring threats, thereby enhancing

situational awareness. Drones can monitor border areas, identify potential threats, and alert response teams. Additionally, they can strengthen the security of military bases and improve the safety of military in combat.

Electronic warfare: AI can be utilized to analyze radio signals and other forms of electronic communication to identify enemy positions, disrupt their communication networks, and gain a tactical advantage over opposing forces.

Combat training simulation: Military training simulation software has become widely used in the AF. By integrating AI, digital models are created that prepare military for the use of combat systems during exercises and operations. In essence, military training simulation offers a virtual "war" environment, providing military with realistic missions and tasks. This allows them to gain valuable experience and before applying their skills in actual combat situations.

Military education and educational programs: AI can improve military training and educational programs by using advanced language models generated by it to introduce new training materials. It can also assess students' current skills, and tailor training to their specific needs. Additionally, conversational AI can provide personalized feedback to help students develop their skills, while also assisting commanding officers in identifying areas where individual students may be struggling.

While AI holds significant potential for military training applications, it should never fully replace human instructors. Instructors are responsible for determining the overall curriculum, while AI can create personalized lessons tailored to individual needs, which human instructors can then review for accuracy and other issues. With AI's assistance, instructors can develop and administer more effective training programs by providing individualized attention to students - something that may be difficult to achieve in terms of speed and quality without AI support.

Target recognition and classification: AI can significantly improve target recognition in combat environments, accurately identifying vehicles, aircraft, ships, combat systems, supply bases, personnel, and more. By rapidly collecting, examining, and analyzing reports, documents, news, and other forms of information, AI enables defense forces to gain a comprehensive understanding of an operational area much faster than humans can. AI systems also have the ability to predict enemy behavior, identify vulnerabilities, assess weather and environmental conditions, evaluate mission strategies, and propose execution plans. This can save time and human resources by allowing military to stay ahead of their targets. However, as always, final decisions must remain with humans.

Cybersecurity: Even highly secure military systems are vulnerable to cyberattacks, where AI can be of great help. Cyberattacks can compromise classified information or disrupt systems, endangering military personnel and jeopardizing mission success. AI can safeguard programs, data, networks, and computers from unauthorized access. Additionally, AI can analyze cyberattack patterns and develop defensive strategies to mitigate them. These systems are capable of detecting the smallest signs of an attack

before it infiltrates a network. Scenario generation and enhanced communication capabilities also bolster cybersecurity in military environments. By analyzing large volumes of data and identifying patterns, AI can detect and neutralize potential threats, using predictive analytics to forecast and prevent future attacks.

Logistics, supply and transportation management: AI can significantly improve logistics operations by optimizing route planning, inventory control, and resource allocation, ultimately enhancing efficiency and reducing costs. Logistics and transportation are critical to the success of military operations, and AI can play a vital role in the transportation of ammunition, goods, weapons, and troops. By determining the most efficient routes based on current conditions, AI helps reduce transportation costs and minimizes the need for human input. Additionally, AI can proactively identify potential issues with military fleets in order to ensure optimal performance.

Medical diagnosis and treatment: In combat situations, doctors, like other military personnel, are often required to make quick and crucial decisions under pressure. AI can assist medical personnel by analyzing injury cases, diagnosing conditions, prescribing treatments, and providing tailored care in these challenging environments. This process provides access to data containing medical trauma cases, which include diagnoses, vital sign sets, medications, records, treatments, and outcomes. This data is then combined to provide indications, warnings, and treatment suggestions. While AI is not qualified to make final medical decisions, it provides rapid analysis and provides doctors with additional information to support their decision-making.

5. Companies applying artificial intelligence in the defense sector[9]

Some of the most powerful U.S. companies that are using artificial intelligence technology in the field of defense are:

1) **Anduril**, develops defense equipment such as: drones, and surveillance towers that are integrated into a common software platform known as "Lattice OS".
2) **Rafael,** is an Israeli company recognized as the National Defense Laboratory, specializing in the development of military weapons and technologies within Israel's Ministry of Defense.
3) **L3Harris,** It is a leader in military aviation, equipped with electronic systems to provide reliable solutions for military challenges for the United States and its allies.
4) **Palantir,** helps the U.S. military use AI insights to make rapid decisions in multiple areas to fulfill the mission. This ensures that data is accessible at all levels for fast and secure decision-making.
5) **Grupi Thales**, is a multinational defense and aerospace company that provides advanced technological solutions in the fields of AI, cybersecurity and autonomous systems.

[9] Marcus Law, Technology Magazine, 7 March 2023.

6) **IBM,** Headquartered in Armonk, New York, IBM is an American multinational technology corporation with a presence in over 175 countries. It can help government departments and corporations transition to an advanced hybrid cloud-based environment built on technology that is designed to fulfill its mission.

7) **Raytheon Technologies,** is a multinational defense and aerospace company that provides advanced technological solutions in the fields of cybersecurity and electronic warfare.

8) **Northrop Grumman,** is an U.S national aerospace and defense company that designs, develops, builds and supports the world's most advanced products, including cutting-edge aircraft, spacecraft, cybersecurity systems, radars, etc.

9) **Lockheed Martin,** is an U.S aerospace, weapons, defense, information security and technology corporation with global interests. It was founded in March 1995 by the merger of Lockheed Corporation and Martin Marietta. It is headquartered in North Bethesda, Maryland, D.C. Last year, the corporation announced the launch of the first version of its AI Factory, an internal ecosystem designed to develop and produce AI solutions.

10) **BAE systems,** is a multinational defense, security, and aerospace company, which works on advanced technologies in AI, cybersecurity, and electronic warfare.

6. Advantages and disadvantages

Advantages and disadvantages of applying AI in various fields of human activity:

Advantages:

- Processes data, makes more accurate predictions than humans as well as facilitates the work of researchers.
- Solves difficult data, does oriented and highly detailed work compared to humans.
- Provides consistent results and increases productivity.
- Increases transparency and influences decision-making.
- Saves manpower.
- Virtual AI Agents are available around the clock (24/7).

Disadvantages:

- Provides expensive service due to high cost of computer tools.
- Requires deep technical expertise which is provided by a limited number of qualified personnel.
- Reflects biases in data management, increasing the degree of their manipulation.
- There is no creativity, limiting thought and action in the broad spectrum of life,

increasing the extent of passivity in daily activity.

- Eliminates jobs, increasing the unemployment rate.

Advantages and disadvantages of AI application in the field of defense:

Advantages:

- AI has the potential to revolutionize global military affairs, constituting a technological revolution with an impact on the international strategic balance, making it the subject of intense debate.
- The careful application of AI can improve the functioning of many aspects of military operations, increasing productivity and reducing human impact.
- AI uses information collection and analysis methods to provide guidance and direction that help military leders improve their understanding of the operational environment, reduce the cognitive load of the situation, and support them in making the right decisions for the successful accomplishment of the mission.
- The use of AI enables humans to delegate high-risk tasks to non-human agents, which increases the level of security for their protection.

Disadvantages:

- The risks associated with the use of AI in military applications are multifaceted and require careful consideration and comprehensive solutions.
- Since AI requires a vast amount of data to handle, it can be vulnerable to manipulation. On this basis, additional protective measures are required in order to cope with threats.
- The application of AI raises concerns about reducing the critical role of judgment or losing human control over the use of combat equipment, leading to inciting conflicts, committing acts inconsistent with international humanitarian law, and avoiding accountability for irresponsible actions.
- Proliferation of Military AI raises serious concerns about its potential use by non-state actors and rogue nations, who are difficult to manage.

Conclusions

Artificial intelligence is undoubtedly opening new horizons in defense technologies, with high expectations for its application across numerous military domains. However, certain limiting factors and unresolved issues still require further research to meet the expectactions. Analysis indicates that rather than fostering skepticism about AI's broad applicability, this situation highlights the need for increased intellectual effort and financial resources dedicated to research and development. Recent advancements in AI are reshaping defense and global security for the EU and NATO's countries. To fully harness these technologies, it is essential to establish suitable regulatory and ethical frameworks, increase investment in research and

development and strengthen international cooperation. This approach will enable responsible and effective use of AI to enhance global defense and security.

Recommendations for the development and use of Artificial Intelligence in the Armed Forces

Human resource management: AI can be leveraged to modernize the entire human resource management system, covering the full lifecycle of military personnel, from recruitment and assignment to training, social support, promotion, discharge, and retirement.

Education and training: AI should be used to design and implement educational and training programs for military personnel, focusing on the use and maintenance of advanced AI technologies. These programs should aim to automate communication processes and enhance teaching and assessment. Additionally, fostering continuous education will help ensure that military staff remain current with the latest technological advancements and evolving tactics, with updates to curriculum design, teaching methods, and knowledge assessment.

Development of military policies, strategies, and doctrines: Adapting artificial intelligence technology in the AF, requires addressing key issues related to its efficient use, ensuring alignment with ethical standards and information security protocols. Integrating AI capacities into military strategies and doctrines, as well as into planning and decision-making processes will enhance the effectiveness and readiness of the Armed Forces.

Integration of artificial intelligence technologies: Adapting AI systems to enhance detection and surveillance through drones equipped with advanced technology is essential for monitoring the environment and identifying threats in real time. The use of AI algorithms will aid in analyzing intelligence and reconnaissance data to identify threat patterns and predict potential actions of adversaries.

Cybersecurity: Investment in cybersecurity infrastructure is necessary to protect military systems and information networks from cyberattacks. AI can be employed to detect anomalies and cyber threats in real time, improving defense against sophisticated attacks.

Improving logistics and support: AI can be utilized to optimize the military supply chain and logistics, ensuring that resources are delivered to the right place at the right time. Implementing AI systems to manage the maintenance and repair of military equipment is crucial for predicting and preventing defects, as well as ensuring operational readiness.

International Cooperation: Expanding cooperation with NATO's allies will facilitate the exchange of knowledge, resources, and best practices in AI and cyber defense. Engaging in joint research and development projects with NATO countries and other EU countries will enable the exploitation of the latest technologies and

innovations, ensuring interoperability in collaborative efforts and enhancing the effectiveness of joint defense measures to this end.

The implementation of the above recommendations can significantly enhance the Albanian Armed Forces operations planning process, and operational capacities, enabling them to better adapt to the evolving challenges posed by technological advancements, global security, as well as to contribute to maintaining peace and stability in the region and beyond. These technological advancements will be very valuable in strengthening national defense, increasing readiness and improving international cooperation within NATO and other EU countries.

Bibliography:

1. U.S. DOD, *Summary of the 2018 Department of Defense Artificial Intelligence Strategy: Harnessing AI to Advance our Security and Prosperity* (Washington, DC: U.S. DOD, 2018), 5. See:https://media.defense.gov/2019/Feb/12/2002088963/-1/-1/1/SUMMARY-OF-DOD-AI-STRATEGY.PDF.
2. "Deputy Secretary of Defense Kathleen Hicks' Remarks: 'Unpacking the Replicator Initiative' at the Defense News Conference (As Delivered)," U.S. DOD, 6 September 2023. See: https://www.defense.gov/News/Speeches/Speech/Article/3517213/deputy-secretary-of-defense-kathleen-hicks-remarks-unpacking-the-replicator-ini/.
3. "DOD Adopts Ethical Principles for Artificial Intelligence", U.S. DOD, 24 February 2020. See: https://www.defense.gov/News/Releases/Release/Article/2091996/dod-adopts-ethical-principles-for-artificial-intelligence/.
4. James Johnson, *Artificial Intelligence and Future Warfare: Implications for International Security*, Defense and Security Analysis 35, no. 2 (2019): 158. See: https://doi.org/10.1080/14751798.2019.1600800.
5. STAND-TO, Divizioni i Mediave Online dhe Sociale (The management of the Online and Social Media Division –OSMD, Zyra e Shefit të Çështjeve Publike (The Office of the Chief of Public Affairs (OCPA). U.S. Army STAND-TO! | Army Organic Industrial Base Modernization Implementation Plan
6. M. L. Cummings, *Artificial Intelligence and the Future of Warfare*, Institute of International Affairs London, London, UK, 2017.
7. C. H. Heller, *The future navy—near-term applications of artificial intelligence*, Naval War College Review, vol. 72, 2019.View at: Google Scholar
8. J. Dalzochio, R. Kunst, J. L. V. Barbosa et al., *Predictive maintenance in the military domain: a systematic review of the literature*, ACM Computing Surveys, vol. 55, 2023. View at: Publisher Site | Google Scholar.

The importance of drones in detecting and extinguishing wildfires

Colonel Msc. David RROKU
Head of Department at the Military Scientific Research Institute

Abstract

This paper addresses the issues on the creation of firefighting drones and their use assessment for emergency response. The drone is intended to support firefighters in dangerous conditions, especially during forest fires when the approaching of the site by people can be difficult and dangerous. The drone is equipped with a thermal camera (a high-resolution camera) and an on-board water tank for extinguishing flames with water. Advanced 3D printing methods and computer simulations were used for the design and development of the drone. The drone's capabilities have been put to the test in a safe environment and the results showed how good it is for fighting fires

The paper continues with a discussion of the potential use of firefighting drones in disaster management and the issues that need to be resolved to enable its safe and efficient use in practical situations. The drone was created primarily to fight fires; is equipped with gas, water sprinklers and fire extinguishers. Its operating range allows it to successfully extinguish flames in large structures and reach great heights. In the experimental setting, a grassland area was intentionally set on fire, and the expanding rate and intensity of the fire were managed by varying wind speed and fuel load. The drones used for this purpose have infrared cameras as well as smoke sensors. The effectiveness of the drones was assessed based on their ability to detect and extinguish flames, as well as how quickly and swiftly they could move through the burning region.

Keywords: drone, firefighters, firefighting equipment, disaster management.

Introduction

As technology advances, new and creative approaches are being developed to address issues and improve safety in a wide range of sectors. Fighting fires is one area where technology has the potential to have a major impact. Any device that would make firefighting safer and more productive for firefighters would be invaluable[1].

Fighting fires is a dangerous and difficult job. The use of drones is an innovative technique being explored for firefighting. In several uses, including aerial photography, delivery services, and even search and rescue operations, drones have already proven very useful. However, the use of drones in firefighting is a very new and unproven application. Even though the idea of firefighting drones is still experimental, it has huge potential advantages. Drones can be equipped with cameras and sensors to quickly and accurately locate hot spots and other potential trouble spots. They can also be used to transport firefighting materials such as water, foam, or even fire-resistant chemicals to the scene of a fire, which can help extinguish flames more quickly and efficiently[2].

The use of drones in firefighting can also contribute to the safety of firefighters. By providing aerial images of the fire and nearby locations, drones can help firefighters detect potential threats and avoid them. In addition, firefighters on the ground can receive real-time information from drones, enabling them to make more informed decisions about where to focus their efforts. Despite the potential advantages of firefighting drones, some issues still need to be tackled. For example, drones must be able to operate in high-temperature situations and withstand exposure to flames and smoke[3].

In addition, they must be able to maneuver through challenging environments such as buildings or forests while avoiding hazards. There are still additional legal and regulatory considerations that need to be addressed. Currently, there are restrictions on where and how drones can be used in firefighting; as a result, their use is highly regulated[4]. However, as the technology continues to grow and mature, it is anticipated that these laws will become more flexible and allow the further use of drones in firefighting operations. In this article, we will study the development of firefighting drones and their potential use in real-world firefighting environments.

---

[1] K. Valavanis, G. Vachtsevanos, "Aplikacionet UAV", "Handbook of Unmanned Aerial Vehicles". Valavanis Springer: Berlin, Germany, vol. 3, pg. 2639-2641, 2015

[2] E. Lygouras, A. Gasteratos, K. Tarchanidis, Mitropoulos, A. ROLFER: " A fully autonomous air rescue support system " Mikroprocess. Microsyst, vol. 61, pg. 32-42, 2018

[3] J. Tomotani, "Use of unmanned aerial vehicles in search operations", J. Geek Stud, vol. 2, pg. 41-53, 2015

[4] E. Lygouras, A. Gasteratos, K. Tarchanidis, Mitropoulos, A. ROLFER: "A fully autonomous aerial rescue support system," Microprocess. Microsyst, vol.. 61, fq. 32-42, 2018

Below, we'll cover the technological challenges that need to be addressed, as well as the legal and regulatory considerations that need to be taken into account. Of course, we'll also look at the different types of firefighting drones currently on the market, along with the advantages and disadvantages of each[5]. Throughout this article, I'll provide updates on the latest developments in firefighting drone technology and share insights from industry professionals. The goal is to provide a comprehensive overview of the potential benefits of firefighting drones, as well as the challenges that need to be overcome to make this technology a reality.

Ecology and human lives are seriously endangered by forest fires[6]. The National Civil Protection Agency estimates that fires have recently increased throughout the territory of the Republic of Albania, burning thousands of hectares of forests and pastures, and endangering many residential homes. Forest fires are becoming increasingly severe and frequent, which highlights the need for creative solutions to stop these disasters. To increase the efficiency and safety of firefighting operations, the use of drones has emerged as a possible alternative[7]. Firefighters can analyze the situation, develop an action plan, and take immediate action with the use of drones that can provide real-time monitoring and surveillance of fires. In this experimental publication, we describe the creation and evaluation of a firefighting drone that aims to support firefighters in hazardous circumstances. The drone has a thermal imaging camera, an onboard water tank for extinguishing flames with water, and a high-resolution camera.

1. Research method

In the fight against wildfires and other large-scale fires, firefighting drones are a crucial tool. These drones can provide firefighters with vital information and assistance, enabling them to extinguish the flames successfully and more safely. One of the main advantages of firefighting drones is their ability to provide real-time data and images from the air[8]. This information can help to better understand the size and extent of the fire, the location of hot spots, and assess potential hazards or difficulties associated with extinguishing the fire. Drones can also be used to deliver supplies, such as water or fire retardant, to areas that are difficult or dangerous for firefighters to reach[9]. Several research gaps may hamper the development and use of firefighting drones. Developing more sophisticated imaging and sensor technologies that can

[5] A. Carrio, C. Sampedro, A. Rodriguez-Ramos, P. Campoy, " A review of deep learning methods and applications for unmanned aerial vehicles ", J. Sens, f. 1–13,2015

[6] E. Petritoli, F. Leccese, L. Ciani, "Reliability and maintenance analysis of unmanned aerial vehicles," Sensors, vol. 18, f. 56-71, 2018.

[7] S. Saponara, "Sensing and connectivity systems for assisted and autonomous piloting and unmanned vehicles", Sensors, voll.18, f. 19-29, 2018.

[8] A. Adam, M. Elmaleeh, Mahmoud, D. "A smart neural network based algorithm for landing control of autonomous unmanned aerial vehicle".

[9] K. Vijayakumar, S. Suchitra dhe P. Swathi Shri, "A secured cloud storage auditing with empirical outsourcing of key updates", Int. J. Reasoning-based Intelligent Systems, Vol. 11, nr. 2, 2019.

provide more accurate information about fires is a crucial area of research work. This includes creating thermal cameras that serve to identify hot spots and applying machine learning algorithms to evaluate fire data in real-time[10].

Another major area of research is creating more effective and efficient delivery techniques for firefighting supplies. This includes developing drones that can carry larger loads and deploying new materials and technology to increase the effectiveness of fire-resistant materials and other firefighting products[11]. Finally, there is a need for additional studies on the safety and reliability of firefighting drones. This includes creating reliable communication and control systems to ensure that drones can be used safely in high-risk environments, as well as employing safety measures to prevent drones from colliding with each other or malfunctioning during firefighting activities[12].

2. Purpose of use

The new goal of firefighting drones is to provide a faster and more effective means of extinguishing fires. Firefighters can make better judgments about how to fight a fire with the use of drones, which can provide real-time information about the location and intensity of a fire. Drones could potentially be used to assist firefighters by transporting tools and supplies such as water or fire extinguishers. Using firefighting drones to reduce the risk to firefighters is another emerging use. Drones can reach places that are too dangerous for firefighters to approach, including burned structures or areas with a lot of smoke[13].

Firefighting drones are used to detect, stop the spread of flames and extinguish fires.

Exploiting drones to monitor the environment for potential fires is another innovative use for firefighting equipment.

Drones can be equipped with sensors that can identify changes in temperature, humidity, and other environmental variables that can increase the risk of fires. Firefighters can use this information to be informed of potential fire hazards so they can take precautions before one starts. To effectively extinguish fires, firefighting drones must overcome several obstacles[14].

---

[10] Hugo Rodrigue, Seunghyun Cho, Min-Woo Han, Binayak Bhandari, Jae-Eul Shim & Sung-HooAhn, Effect of twist morphing wing segment on the aerodynamic performance of UAV, Journal of Mechanical Science and Technology., 2016

[11] Fu-Hsuan Wen, Fu-Yuen Hsiao, and Jaw-Kuen Shiau, Analysis and Management of Motor Failures of Hexacopter in Hover, Department of Aerospace Engineering,2021

[12] Huy X. Pham; Hung M. La; David Feil-Seifer; Matthew Deans, A distributed control framework for a team of unmanned aerial vehicles for dynamic wildfire tracking, 2017 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS)., 2017.

[13] Hugo Rodrigue, Seunghyun Cho, Min-Woo Han, Binayak Bhandari, Jae-Eul Shim & Sung-HooAhn, Effect of twist morphing wing segment on the aerodynamic performance of UAV, Journal of Mechanical Science and Technology, 2016.

[14] Wildfire Causes. Fire and Aviation Management, National Park Service U.S Department of Interior Available online: cfm (accessed on 6 December 2017)

Figure 1. Controlling firefighting drones.

Some of the main challenges include:

- Drones must be able to navigate in a dense and dynamic environment while simultaneously avoiding obstacles and maintaining stable flight. Windy weather conditions can affect the in-flight stability of the drone and create turbulence, which can be quite challenging. Drones used in firefighting must be able to carry a large load, such as water or other firefighting equipment. This requires a powerful engine and battery, which can increase the weight of the drone and shorten the flying time.
- Limited flight time: Drones have limited flight time due to battery life, which can be problematic for putting out fires that need a long time to be extinguished. As a result, drones may have to be used as useful means besides the other firefighting tools such as ground crews or helicopters.
- Drones must be able to withstand both extreme heat and flames while still operating. This can be achieved by using fire-resistant materials and cooling systems, which unfortunately add additional weight and complexity to the drone[15].
- The movements and actions of the firefighting drones must be well coordinated with those of the other resources, as well as ground-based crews, to ensure effective fire suppression. This requires robust communication systems and protocols, as well as skilled operators who can control it in a dynamic environment.

[15] Remington, R.; Cordero, R.; March, L.; Villanueva, D. Multi-Purpose Aerial Drone for Bridge Inspection and Fire Extinguishing. Unpublished Thesis, Florida International University, Miami, FL, USA, 2016. [20] Marchant, W.; and Tosunoglu, S. Rethinking Wildfire Suppression with Swarm Robotics. In Proceedings of the 29th Florida Conference on Recent Advances in Robotics, FCRAR'16, Miami, FL, USA, 12–13 May 2016.

3. Design and Development

The design and development of the drone have been carried out using advanced 3D printing techniques and software simulations. The drone's body consists of lightweight and durable materials, making it capable of withstanding the extreme conditions encountered in firefighting. The drone's rotors and propulsion system were optimized to ensure stability and maneuverability, allowing it to fly through narrow and complex environments. The drone's camera and thermal imaging technology were carefully selected to provide high-resolution images and real-time temperature data of the fire[16].

The onboard water tank is designed to provide a sufficient amount of water for firefighting. The water tank capacity was optimized to balance the drone's weight and flight time, ensuring that it can operate efficiently for a long time. The water tank is equipped with a spray mechanism that can be remotely controlled to adjust the flow and direction of the water. The proposed firefighting drone is designed to operate in various environments including urban, rural, and industrial areas. The drone has a quadcopter configuration, which ensures stability and maneuverability in the air. The drone's frame is made of lightweight, high-strength materials, such as carbon fiber, to reduce weight and increase load capacity[17].

Firefighting drones are an emerging technology being developed to help manage and fight fires. Listed below are several types of firefighting drones that are still under development or have been used experimentally:

- **Drones for monitoring and evaluation:**

Drone with thermal cameras: These drones are equipped with thermal cameras to identify heat sources and assess the spread of fire on the ground. They provide a clear picture of the situation and help emergency teams plan response strategies.

Drones with environmental sensors: Sensors for temperature, humidity, and harmful gases help collect detailed data on fire conditions and help predict its spread.

- **Drones for liquid delivery:**

Drones with usable tanks: These drones are equipped with tanks for firefighting fluids. They can transport and distribute materials to help control fires in hard-to-reach areas.

Drones with rapid delivery systems**:** Such drones use sophisticated mechanisms to deliver specific substances to small, precisely defined areas.

- **Drones for rescue equipment delivery:**

Drones with the capacity to deliver rescue equipment: These drones can deliver

[16] Death and destruction in the Philippines," IFSEC PHILIPPINES, 2019.

[17] Marchant, W.; Tosunoglu, S. Rethinking Wildfire Suppression with Swarm Robotics. In Proceedings of the 29th Florida Conference on Recent Advances in Robotics, FCRAR'16, Miami, FL, USA, 12–13 May 2016.

important equipment such as first aid kits, radios for communication, or protective fencing to isolated areas where emergency teams cannot immediately reach.

***Drones with safe route modes**:* They can use technology to safely navigate and avoid obstacles that occur during operations in difficult conditions.

- **Drones for predicting fire spread:**

***Drones with data analysis algorithms**:* These drones use algorithms and models to analyze data and predict fire spread based on weather conditions, terrain, and fire intensity.

***Drones for simulations and testing**:* Such drones can be used to simulate and test different fire spread scenarios to prepare more effective response strategies.

- **Drones for communication and coordination:**

Drones for communication: These drones provide stable and secure connections for communication between emergency teams to help coordinate operations during crisis situations.

***Drones with navigation assistance systems**:* They help coordinate rescue teams and ensure that aid arrives safely in fire-affected areas.

Each type of drone has different uses and advantages, and selecting the right type will depend on the specific needs of the mission and the conditions on the terrain. Overall, firefighting drones represent a significant step forward in emergency management technology, and can help in saving lives and protecting assets.

4. Assessment of the Drone's Capability to Fly in Difficult Conditions

Firefighting drones' capability to navigate difficult conditions would require a series of tests and evaluations to determine their effectiveness[18]. The following are some factors that can be considered when evaluating a drone's flying capability:

- **Avoiding obstacles:** The drone must be capable of detecting and avoiding obstacles such as trees, buildings, and power lines while flying in difficult conditions.
- **GPS accuracy:** The drone's GPS system must be accurate enough to navigate in areas with poor GPS coverage or interference.
- **Altitude control:** The drone must maintain a stable altitude in changing weather conditions, including strong winds, gusts, and turbulence.
- **Flight stability:** The drone must be able to fly stably in difficult conditions, including headwinds, turbulence.
- **Visual navigation:** The drone must be able to use visual cues to fly in areas where GPS coverage is poor, such as in dense urban areas or forests.

[18] G. Hovland dhe M. Ottestad, " "Optimization of multicopter UAV design", in the 10th International Conference on Mechatronic and Embedded Systems and Applications (MESA), Senigallia, Itali, 2014.

- **Emergency response:** The drone must be capable of responding quickly to emergencies, such as detecting fires and providing real-time data to firefighters on the terrain[19].
- **Battery life:** The drone must be capable of maintaining its hovering ability for a long period, especially during prolonged firefighting operations.

5. Load Capacity

Load capacity is a critical factor to take into consideration when it comes to firefighting drones. It determines the amount of equipment and supplies the drone can transport to the scene of a fire. The load capacity varies depending on the drone's size, design, and weight[20]. To test the load capacity of the firefighting drone, it is necessary to conduct a series of experiments that involve adding different payloads to the drone and observing how it performs. The steps involved in this process are as following:

1. Determining the maximum weight the drone can carry, including its own weight. This information is usually provided by the drone manufacturer.
2. The testing process starts with a light load that is gradually increased until the drone can no longer lift or move without problems.
3. Taking into account the weight of the load that the drone can carry without difficulty. This will be the maximum load capacity of the drone.
4. Repeated testing with different types of loads to ensure the drone can carry various types of equipment and supplies.
5. Preparing a short report that includes the drone specifications, the weight of the loads used, and the results of the experiment, and then requesting according to market needs and prices.

6. Delivery Accuracy

The accuracy of a firefighting drone delivery system designed to drop water will depend on various factors such as: the design of the system, the capabilities of the drone, and the conditions in which it operates. After testing, the accuracy of the system can be assessed based on the success rate of delivering water to the target area. This can be measured using metrics such as the distance between the target area and the actual drop zone, the volume of water delivered to the target area, and the time it takes to complete the delivery. To improve accuracy, the system can be fine-tuned based on test results, adjusting parameters such as the drone's flight path, speed, altitude, and load. Continuous testing and refinement of the system could lead to higher levels of accuracy over time. The drone was found to have a high level of

[19] Guvenc, F. Koohifar, S. Singh, ML Sichitiu and D.Matolak, "Detection, Tracking and Stopping for Amateur Drones", Detection, Tracking and Stopping for Amateur Drones, Vol. 56, No. 4, pg. 75-81, 2018

[20] Maya, M., Castillo, E., Lomelí, A., GonzálezGalván, E., & Cárdenas, A. (2013). Workspace and payload-capacity of a new reconfigurable delta parallel robot. International Journal of Advanced Robotic Systems, 10(1), 56

delivery accuracy, capable of water-dropping, fire-resistant precision targeting targets of various sizes and shapes.[21] The drone's load capacity is shown in the figure below.

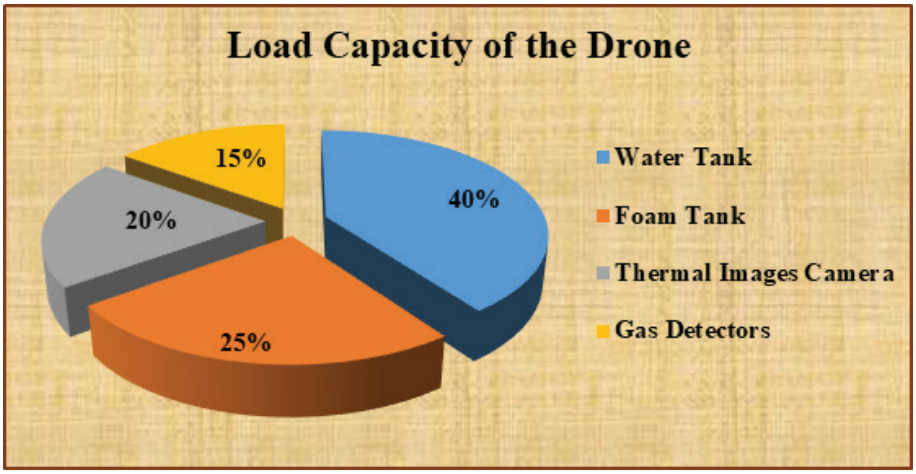


Figure 2. Load capacity of the drone.

7. Flight Time and Range

The firefighting drone's flight time and range can vary depending on several factors, such as the drone's battery capacity, weight, weather conditions, and load capacity. Upon testing process completion, the flight time and range of a firefighting drone can be determined based on its specific specifications and capabilities.

For example, a drone with a larger battery capacity can typically fly for a longer time than one with a smaller battery. Similarly, the range of a drone can also be affected by its weight and weather conditions. A heavier drone may not be able to fly as far as a lighter drone, and strong winds or other environmental factors can reduce the drone's range. Generally, firefighting drones are designed to have a flight time of around 20-30 minutes and a range of up to several kilometers. However, the exact flight time and range will depend on the specific drone model and its individual capabilities. The drone was found to have a flight time of up to 25 minutes and a range of up to 2 kilometers.[22].

8. Fire Extinguishing Efficiency

It has been established that drones are very effective in extinguishing fires in various types of environments. The drone is capable of quickly extinguishing fires of various

[21] Deng, L., He, Y., & Liu, Q. (2019, October). Research on application of fire unmanned aerial vehicles in emergency rescue. In 2019 9th International Conference on Fire Science and Fire Protection Engineering (ICFSFPE) (pp. 1-5). IEEE.

[22] Zadeh, N. R. N., Abdulwakil, A. H., Amar, M. J. R., Durante, B., & Santos, C. V. N. R. (2021). Firefighting UAV with shooting mechanism of fire extinguishing ball for smart city. Indones. J. Electr. Eng. Comput. Sci, 22, 1320-1326

sizes and shapes. Firefighting drones are unmanned aerial vehicles (UAVs) equipped with firefighting capabilities such as water, foam, or other chemicals.

Testing of these drones typically involves evaluating firefighting effectiveness in controlled environments to assess their ability to put out fires efficiently and safely[23]. During testing, firefighting drones are typically subjected to various fire scenarios, including small fires, large fires, and different types of fires (such as electrical fires or chemical fires). The drones are then tasked with extinguishing the fires using their onboard firefighting equipment. Test results typically focus on the drone's ability to effectively extinguish a fire, as well as its speed and efficiency in doing so. Factors such as the amount of water or other extinguishing agent used, the distance between the drone and the fire, and the accuracy of the drone's targeting system can all be considered when evaluating a drone's performance.[24]

The testing can also assess the drone's ability to navigate through smoke and other obstacles to reach the fire, as well as its overall durability and reliability under various operating conditions. Overall, the test results can provide valuable insights into the performance of firefighting drones and help improve their design and functionality. By evaluating their effectiveness in controlled environments, researchers and engineers can identify areas for improvement and optimize their performance for use in real-world firefighting scenarios[25].

Conclusions

This article presented the development and testing of a drone designed to assist firefighters in hazardous situations. The drone was designed and developed using advanced 3D printing techniques and software simulations, resulting in a lightweight and durable drone capable of withstanding extreme conditions.

The drone's capabilities were tested in a controlled environment, demonstrating its effectiveness in extinguishing fires. Firefighting drones have significant potential applications in disaster management. They can provide real-time monitoring and surveillance of fires, helping firefighters develop and take concrete measures to eliminate fire. Based on the experimental data on the use of firefighting drones, we reach the following conclusions:

- Firefighter's drones can significantly improve the effectiveness and efficiency of firefighting operations by providing an innovative solution.

[23] Borthakur, A., & Singh, P. (2016). Drones: new tools for natural risk mitigation and disaster response. Current Science, 110(6), 958.

[24] Alappatt, T. B., Ajith, S. S., Jose, J., Augustine, J., Sankar, V., & George, J. M. (2021). Design and Analysis of Fire Fighting Drone. In Advances in Electrical and Computer Technologies: Select Proceedings of ICAECT 2020 (pp. 1015-1033). Springer Singapore.

[25] Barua, S., Tanjim, M. S. S., Oishi, A. N., Das, S. C., Basar, M. A., & Rafi, S. A. (2020, June). Design and implementation of fire extinguishing ball thrower quadcopter. In 2020 IEEE region 10 symposium (TENSYMP) (pp. 1404-1407). IEEE.

- The use of drones in firefighting operations can reduce the risk of injury to firefighters by eliminating the need for them to enter dangerous areas.
- Drones equipped with thermal imaging cameras can quickly identify hot spots and provide firefighters with real-time data, allowing them to make informed decisions and adjust their strategies accordingly.
- The use of drones in firefighting operations can also reduce response times by quickly assessing the situation and allowing for faster deployment of resources.
- Firefighting drones have already passed the experimental stage and do not require further testing and development to become a standard tool in firefighting operations.
- Challenges such as battery life, range, and load capacity need to be addressed to improve their effectiveness and use.
- Drones can help firefighters access and assess fire situations quickly and safely and provide valuable data and intelligence to help inform firefighters on firefighting strategies. Experimental analysis has shown that drones equipped with thermal imaging cameras can effectively detect hot spots and provide real-time feedback to firefighters. Furthermore, the drones' use can also aid in search and rescue efforts, as they can quickly scan large areas and identify any individuals needing assistance.

However, there are also some limitations and challenges that need to be addressed. For example, drones are susceptible to interference from other wireless signals and can be affected by adverse weather conditions such as strong winds and rain. Furthermore, the battery life of drones can limit their operating time and range.

In conclusion, the analysis of firefighting drones has highlighted their potential to improve firefighting operations and increase safety for firefighters. While there are still some challenges to overcome, continued research and development in this area could lead to improvements in firefighting drone technology.

References:

1. A. Adam, M. Elmaleeh, Mahmoud, D. "A smart neural network based algorithm for landing control of autonomous unmanned aerial vehicle," Int. J. Adv. Res. Sci. Eng, vol. 6, pp. 1175–1188, 2018.
2. Alappatt, T. B., Ajith, S. S., Jose, J., Augustine, J., Sankar, V., & George, J. M. (2021). Design and Analysis of Fire Fighting Drone. In Advances in Electrical and Computer Technologies: Select Proceedings of ICAECT 2020 (pp. 1015-1033). Springer Singapore.
3. B. Aydin, E. Selvi, J. Tao and M. J. Starek, "Use of Fire-Extinguishing Balls for a Conceptual System of DroneAssisted Wildfire Fighting," MDPI (drones), vol. 3, no. 17, 2019.

4. Barua, S., Tanjim, M. S. S., Oishi, A. N., Das, S. C., Basar, M. A., & Rafi, S. A. (2020, June). Design and implementation of fire extinguishing ball thrower quadcopter. In 2020 IEEE region 10 symposium (TENSYMP) (pp. 1404-1407). IEEE.

5. Burchan Aydin, Emre Selvi, Jian Tao and Michael J. Starek, "Use of Fire-Extinguishing Balls for a Conceptual System of Drone-Assisted Wildfire Fighting", Published: 12 February 2019.

6. Cervantes et al., "A Conceptual Design of a Firefighter Drone," in 2018 15th International Conference on Electrical Engineering, Computing Science and Automatic Control (CCE), Mexico City, Mexico, 2018.

7. Daniel Lawrence I, Vijayakumar R, Agnishwar J, (2023). Dynamic Application of Unmanned Aerial Vehicles for Analyzing the Growth of Crops and Weeds for Precision Agriculture. Artificial Intelligence Tools and Technologies for Smart Farming and Agriculture Practices. Pages: 115-132. DOI: 10.4018/978-1-6684-8516-3.ch007.

8. Death and destruction in the Philippines," IFSEC PHILIPPINES, 2019.

9. Deng, L., He, Y., & Liu, Q. (2019, October). Research on application of fire uumanned aerial vehicles in emergency rescue. In 2019 9th International Conference on Fire Science and Fire Protection Engineering (ICFSFPE) (pp. 1-5). IEEE.

10. E. Lygouras, A. Gasteratos, K. Tarchanidis, Mitropoulos, A. ROLFER: "A fully autonomous aerial rescue support system,"Microprocess. Microsyst, vol. 61, pp. 32–42, 2018.

11. E. Petritoli, F. Leccese, L. Ciani, "Reliability and maintenance analysis of unmanned aerial vehicles," Sensors, vol. 18, pp. 56-71, 2018.

12. Fuller, S. B. (2019). Four wings: An insect-sized aerial robot with steering ability and payload capacity for autonomy. IEEE Robotics and Automation Letters, 4(2), 570-577.

13. J. L. Mayuga, "Tragedy of fires: Death and destruction in the Philippines," The Broader Look, 21 march 2018.

14. J. Manley, "The Comeback of Fire Extinguishing Balls and their Benefits," fire extinguisher pp. 101, 2019.

15. Jeyavel, J., Prasad, A. A., Shelke, K. M., Sargade, P. D., &Thoke, U. V. (2021, March). Survey on firefighting techniques using unmanned aerial vehicles. In 2021 International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE) (pp. 239-241). IEEE.

16. K. Vijayakumar, S. Suchitra and P. Swathi Shri, "A secured cloud storage auditing with empirical outsourcing of key updates", Int. J. Reasoning-based Intelligent Systems, Vol. 11, No. 2, 2019.

17. Kostoulas, P., Oteafy, S., &Chatzimisios, P. (2022, May). Fire-Fighting Drones: A Use Case for Tactile Internet. In ICC 2022-IEEE International Conference on Communications (pp. 4613-4618). IEEE.

18. Parkavi G, Daphine Desona Clemency C A, Rehash Rushmi Pavitra A, P. Uma Maheswari, I. Daniel Lawrence, 2023. Internet of Things (IoT) Enabled Cloud Computing Drone for Smart Agriculture: Superior Growth and Life. Journal of Population Therapeutics and Clinical Pharmacology, 30(12), pp.256-262.

19. Rehash Rushmi Pavitra A, Parkavi G, Uma Maheswari P, Karthikeyan K, Daniel Lawrence I, 2022. An Illustrative Review on Machine Learning Techniques along with Software Tools and its Evaluation. NEUROQUANTOLOGY, 20(16), pp.233-236.

20. S. H. Alsamhi, O. Ma, S. M. Ansari, and S. K. Gupta, "Collaboration of Drone and Internet of Public Safety Things in Smart Cities: An Overview of QoS and Network Performance Optimization," MDPI, vol. 3, 2019.

21. T. Markarian,"Unmanned aerial vehicles (drones) to prevent drowning", Resuscitation, vol. 127, pp. 63-67, 2018.

22. Vijayakumar, S. Suchitra and P. Swathi Shri, "A secured cloud storage auditing withempirical outsourcing of key updates", Int. J. Reasoning-based Intelligent Systems,Vol. 11, No. 2, 2019.

23. Y. LeCun, Y. Bengio, G. Hinton. "Deep Learning," Nature, vol. 521, pp. 436–444, 2018.

24. Yao, Q., Qiu, J., Fan, Y., & Yan, W. (2021, May). Quad-rotor fire-fighting drone based on multifunctional integration. In 2021 International Conference on Artificial Intelligence and Electromechanical Automation (AIEA) (pp. 70-73). IEEE.

25. Yuan, C.; Zhang, Y.; Liu, Z. A survey on technologies for automatic forest fire monitoring, detection, and fighting using unmanned aerial vehicles and remote sensing techniques. Can. J. For. Res. 2015, 45, 783–792.

26. Yuan, Y. (2021, April). Technical Research on Fire- Fighting Robotics. In 2021 IEEE Asia-Pacific Conference on Image Processing, Electronics and Computers (IPEC) (pp. 140-143). IEEE.

27. Z. Guowei, Y. Su, Z. Guoqing, F. Pengyue and J. Boyan, "Smart firefighting construction in China: Status, problems, and reflections," FAM fire and materials an international Journal, vol. 44, no. 4, no. 2020 John Wiley & Sons Ltd, pp. 516-529, 22 January 2020.

28. Zadeh, N. R. N., Abdulwakil, A. H., Amar, M. J. R., Durante, B., & Santos, C. V. N. R. (2021). Fire- fighting UAV with shooting mechanism of fire extinguishing ball for smart city. Indones. J. Electr. Eng. Comput. Sci, 22, 1320-1326.

Quantum technology and its information security

Colonel Msc. Ulsi REXHAJ
Director of the Military Scientific Research Institute

Abstract

Today's opportunities and communication skills, critical thinking, and the integration of quantum technology in security systems has become increasingly widespread concerning storage of basic data, information administration, management and circulation. This article examines the impact of quantum technology, which is based on the laws of quantum mechanics, on quantum security, as a necessity of time, regardless of financial costs.

The findings show that the different forms of classical technology used so far affect the security results of the preservation of critical data infrastructure, information and their circulation. However, an active engagement in quantum technology will have a profound impact on quantum security experiences, reflecting increased motivation, improved security capabilities, and improved access to basic resources.

The extent of integration of this technology compared to the classical one plays an important role in determining the results, being used strategically to maximize its positive effects, with the aim of debuting in a technology-driven world.

Key words: Quantum technology, quantum security, binary security, laws of physics, encryption, cyber attack, data, information administration, algorithms, protocols, interference etc.

Introduction

Preservation of networks and information is one of the most important topics related to today's developments, long-term competitiveness and achieving global security. The term "quantum security" derives from quantum technology based on the laws of quantum mechanics, which indicates a rational, integral, homogeneous function of two or more variables.

Network security and information storage refer to all measures we take to prevent any data loss or network intrusion that can be caused by user errors, code defects, malicious activities, hardware failure or natural causes. In other words: security and the measures for its implementation are an imperative necessity of the time. This represents the process by which a domain, a product or a service is preserved, renewed and updated by applying new methods, introducing contemporary techniques or developing successful ideas to create new values of work organization, service, management etc. Among organizations and institutions, there are many employees who are not sufficiently familiar with security issues, therefore they can pose a risk to the flow of information and the management of networks. Today, it is not difficult to find different tools, devices and programs, which are essentially designed for good purposes "for the protection and control of networks", but which hackers or different attackers can use to penetrate into the networks of an organization, institution or, in their entirety, for various destructive purposes.

Technology innovation can be an essential driver of security development by seeking to be continually more successful, replacing classical technologies with quantum technologies and transitioning classical/binary security to quantum security. To be successful, we must be able to identify opportunities and take advantage of them. Only by examining and evaluating the security we have and ascertaining what security we need today and, in the future, will we be able to stay ahead of its growing trends, as well as be willing to experiment with new ideas.

For thousands of years, code-makers and code-breakers have competed for supremacy. Their arsenals are beginning to include a powerful new weapon: quantum mechanics. Cryptography or the "art of code-making" has a long history of military and diplomatic applications, dating back to the Babylonians. Nowadays, it is becoming more and more important in commercial applications for e-business and e-commerce. Sensitive data, such as credit card numbers and personal identification numbers (PINs), are routinely transmitted in encrypted form. Quantum mechanics is a new tool for both code breakers and code makers in their eternal race. It has the potential to revolutionize cryptography both by creating perfect secure codes and by breaking standard encryption schemes.

1. Use of Quantum Technology in Daily Life

Quantum technology is a class of technology that operates by using the principles of quantum mechanics (subatomic particle physics), including quantum entanglement

and superposition. The reason we are focusing on quantum technology now, 50 years after it became a part of our lives through nuclear energy, is that the latest engineering achievements are making more use of the potential of quantum mechanics. This technology is used in quantum sensors and computers being developed through quantum engineering that is based on the laws of quantum mechanics. Currently, both entanglement and quantum superposition are being controlled, making it a fascinating field that uses the principles of quantum physics to create new and powerful tools. Unlike classical technology, particles are used at the subatomic level to achieve things that were previously unimaginable. This means it promises improvements on a wide range of daily devices, including:

- More reliable navigation and timing systems.
- More secure communications.
- More accurate healthcare imaging through quantum sensing.
- More accurate and powerful calculations.

The most useful ones in daily life are:

- Quantum magnetometer in medicine, which uses quantum effects to detect the smallest changes in the magnetic field, e.g., MRI (magnetic resonance imaging) scanners.
- Quantum cryptography in data security, using quantum particles, such as photons, to transmit information, it provides a high level of security for our data.

Quantum technology is not only the future, but it is already a reality that is changing the way we understand and use the world around us. Through today's applications we anticipate what the next steps in quantum progress will bring and how they will lead us to new horizons. All these applications can be useful in the short term, but it is difficult to know what will be a true evolution and what will be destructive. This uncertainty indicates that the difference between evolution and revolution is likely to be an early investment.

2. Benefits and Potential of Quantum Security

Quantum security is a security paradigm in the field of information that uses the concepts of quantum physics to ensure the communication and exchange of information in a way that is undetectable and unimaginable by third agents, even though they may have control over the data in transmission. One of the ways to achieve this is through the use of connected quantum cultures. In this case, quantum communication can be done through polarized light representing quantum bits. Using quantum security protocols such as the BB84 protocol, information is encoded in these bits that can represent secure data.

Also, another way is through the community of protected cores. Here, information is encoded in the states of a selected quantum device, for example, the spin states of an atom or photon. During quantum communication, if any attempt occurs to receive or

distribute information from an outsider, the quantum information inviolability effect will cause the attempt to be exposed. This is based on the law of quantum physics, that an attempt to extract information from a quantum system will affect its state. To enable quantum security in practice, quantum community technologies are needed, which are already being developed in scientific laboratories around the world. These technologies aim to provide an impartial and secure way to communicate between parties, exploiting the precise qualities of quantum physics to ensure data integrity and privacy. Quantum security is useful because it provides:

Inviolability of information. In quantum systems, information is secure due to the quantum characteristics of the devices, making visible the attempts to tamper with or record the information.

Conveyance of interference or misdemeanors. If a third party attempts to record or monitor a quantum communication, the inviolability effect affects the state of the information and indicates that tampering has occurred.

Asymmetric security. In most quantum security protocols; participants can distribute a secure hash of keys without questioning their integrity. This creates an asymmetric key distribution that is difficult for attackers to exploit.

Elimination of security breach attempts. The inviolability and storage effect of quantum information can defeat attempts to breach security, making attackers think twice before attempting to exploit a quantum system.

Security at a physical level. Quantum security is based on the laws of quantum physics, such as superposition and the inviolability interaction, which renders it the foundation of security and independent of computer algorithms or other sciences that may have security limitations.

Potential use for important applications. Quantum security can be applied in various fields where security is critical, such as telecommunications, banking, health systems and computer science.

For these reasons, quantum security has the potential to change security paradigms, making them more secure and reliable, due to its unique benefits from the characteristics of quantum physics.

3. Binary Security and its Weaknesses

Binary security is a concept related to the security of data sent and stored through systems and protocols based on binary information. This includes various data security methods, including encrypted data, digital signatures, authentication and access control. It uses tools and methods to ensure that programs are not manipulated and exploited. These tools are not foolproof, but when used together and implemented properly, they can greatly increase the difficulty of exploitation. Some of the methods used for binary security include:

- No Execution (NX):

The No eXecute or NX bit, also known as data execution prevention (DEP), marks certain areas of the program as non-executable, meaning that input or stored data cannot be executed as code. This prevents attackers from being able to switch to custom shellcode that is stored on the stack or in a global variable.

- Randomization[1] of address space extension:

Address Space Layout Randomization (ASLR) is the randomization of the space in memory containing the program and the shared data. It makes it difficult for an attacker to exploit a service, since its knowledge cannot be reused between program launches.

- Relocation Read-only option:

Relocation read-only (RELRO) is a security measure that makes some binary sections read-only. There are two RELRO "modes": partial and full.

- Placement of notifications/advertisements (Canaries/Cookies):

Stack Canaries are a secret value set in files that changes every time the program starts. Before the function returns, they are checked and if it appears to have been modified, the program exits immediately. This is determined when the program starts for the first time, which means that if the program splits, it keeps the same set of cookies, through a mechanism known as "forking".

But binary security, or security based on ordinary data communication, has some major weaknesses or shortcomings as it is vulnerable to:

- Cryptographic attacks:

Binary encryption algorithms are vulnerable to cryptographic attacks such as brute force, differential analysis, frequency analysis, and others that can exploit the structure of encryption algorithms.

- Unwanted exploits:

Binary security can be affected by unwanted cryptographic attacks, such as backdoors, weak key attacks, and other attacks that can take advantage of weaknesses in the implementation of encryption algorithms.

- Information Transfer:

Encrypted information can be accessed by third parties due to loss of keys, their misuse, or use of weak encryption algorithms.

- Insider Threat:

Internal personnel who have access to binary security systems can be a potential risk to reveal or misuse encrypted information for unintended purposes.

- Information routing (circulation) processes:

Encrypted information may be compromised during data transmission over public

[1] The process of ranking or comparing people, things, issues, evidence, etc.

networks, storage on third-party servers, and their exchange between different applications.

- Communication protocols:

Common communication protocols may have security vulnerabilities that can be exploited to compromise transmitted data, including man-in-the-middle attacks and others that affect the integrity and confidentiality of information.

For these reasons, binary security is not sufficient for applications that require a high level of security and privacy. Therefore, the use of quantum security technologies and other security paradigms has become increasingly preferred to guarantee data protection in today's risky communication and information exchange environments.

4. Quantum Security and Binary Security for Electronic Information Security

Quantum security and binary security are two different approaches to securing information in the computing world.

Quantum security:

- It is based on the principles of quantum physics to create shielded cores, which are untouchable and uncatchable.
- It uses shielded cores to make the information transfer encrypted, making it impossible to tamper with the information and undetectable.
- It takes advantage of the unique properties of matter at the quantum level, such as polarization of light and entanglement[2].
- It provides a level of security that is virtually impossible to penetrate with conventional methods.

Binary Security:

- It is based on algorithms and protocols designed to protect information by encrypting it in certain ways.
- It uses discrete math methods to encrypt and decrypt information, using algorithms such as AES, RSA, and many others.
- It is based on the complexity of cryptographic algorithms and the difficulty of factoring large numbers in mathematics.
- Compared to quantum security, binary security is fragile and can be broken if the encryption algorithms are broken or if there is any delay in their processing.

Differences between quantum security and binary security.

The main difference between them is in the basis, methods and tools that each uses,

[2] Confusion, plexus

but there are also some other differences between quantum security and binary security:

- Information security:

Quantum security is based on the principles of quantum physics and provides an absolute level of security due to the unique characteristics of small matter. On the other hand, binary security is based on mathematical algorithms and protocols and offers a security tailored according to the level of complexity of the algorithms and the value of the key used.

- Information management agility:

Implementing quantum security is more difficult and requires deep knowledge of quantum physics and shielded core technology. Whereas, binary security is more familiar and easier to understand and implement for IT organizations and communities.

- Usage rate:

Binary security is widely used in today's digital infrastructures, such as the Internet, banking and business communications. On the other hand, the implementation of quantum security is still in the development stage and has been mainly used in scientific and experimental fields, however, it is being prepared to use in other fields in the future.

These differences reflect the different nature and challenges of each approach to securing information in the computing world.

5. Methods and Techniques to Protect Data from Harm and Third Parties

When we refer to binary security, we generally mean the methods and techniques used to ensure that data is not only unharmed but also inaccessible to unwanted third parties, these include:

- Data encryption:

The process of changing data into an indecipherable form for anyone who does not have the key to share this information. Encryption can be used to protect data confidentiality through various encryption algorithms.

- Authentication:

Ensuring that a person or system is properly identified before granting access to desired data or resources. This may include the use of passwords, digital certificates or other authentication methods.

- Access control:

Ensuring that only authorized persons or systems have access to specific data or resources. This includes the use of security policies, white lists to control access, and role-based authentication technologies.

- Digital signatures:

Using a given digital signature to verify the origin and authenticity of a document or message. Which can be used to ensure that a message has not been tampered with and comes from the correct source.

These are some of the main aspects of binary security that are used to protect data in computer networks, electronic communications, and numerous information systems that are exposed to the risk of misuse or various attacks.

Challenges and difficulties in applying binary security to quantum technology.

During the application of binary security in quantum technology we encounter several challenges and difficulties, some of which are:

- Complexity of protocols:

Quantum security protocols are complicated and difficult to implement in practice. In-depth knowledge of quantum physics and security algorithms is required, as well as the ability to develop specialized devices that communicate quantumly.

- Adaptation to existing infrastructure:

The implementation of quantum security requires significant investments in new infrastructure and specialized equipment, or in the integration of systems with existing infrastructure.

- Lack of standardization:

In the field of quantum security, there is still no general standard for protocols and technologies, creating difficulties in their selection and implementation.

- Technological limitations:

Quantum technologies are still developing and have their limitations regarding distance, transmission speed, and device stability. Only for some applications it becomes possible to implement quantum security.

- Information processing:

Quantum information requires a new approach to computer science and programming. The development of suitable algorithms for its processing is in the early stages and still challenging for programmers and software engineers.

- Access security:

Achieving access security for quantum systems means eliminating the impact of external interference and attempts to disconnect or monitor communication.

To address these challenges, it is important for the entire scientific and industrial community to continue to invest in the development of quantum technologies, to create common standards and protocols for quantum security.

Applying quantum security to non-quantum computers.

Quantum security uses shielded cores to achieve encrypted communication that cannot be broken without being dictated. To use this technology, we must have

a device that is capable of processing and performing other quantum operations through these cores. So, if the devices we use are not quantum, then we will not be able to use quantum security services which is one of the main advantages of research in the field of quantum computing, but to take advantage of it, specific devices are needed.

Connection between classical and quantum techniques

Classical and quantum techniques are two different approaches to describe and understand the world and its processes. Both together influence modern science and technology in different ways but have a close connection between them in several aspects:

- Theoretical basis:

Classical and quantum techniques are built on different theoretical foundations. The classical aspect is based on classical logic and mathematics, while the quantum one uses concepts and principles of quantum mechanics.

- Interpretation of information:

The classical technique uses binary systems based on the numbers 0 and 1 to describe and manipulate information. Whereas the quantum one uses shielded nuclei and quantum states to describe information and manipulate it in various ways.

- Distribution and exchange of information:

In the classical technique, information is distributed and exchanged through clear communication channels. In quantum, information is linked in an unusual way through quantum nuclei and cells, enabling secure transmission of information.

- Technological implementation:

Classical engineering is used to develop a wide range of technologies, including computers, telecommunications, etc. While the quantum one is used to develop technologies such as quantum computers, quantum security systems, etc.

- Challenges and potentials:

The quantum technique offers several advantages over the classical technique, including higher performance in some applications and greater security in many contexts. However, there are also challenges in implementing and using quantum technology, as in some cases, classical techniques may be more suitable or easier to use.

6. Infrastructure Elements for Quantum Technology

Despite the fact that quantum technology is a new growing domain, several key elements of the infrastructure for this technology have already been created:

- Qubit (quantum bit):

In a quantum computer, the qubit is the basic unit of information in quantum computing analogous to the bit in a classical computer. It can be in a state of

superposition of many possible states of the quantum core, offering the potential to process information in advanced ways.

- Quantum key distribution devices (QKD):

Secure quantum core devices are the centerpiece of the quantum key distribution infrastructure. Through the use of quantum phenomena, such as polarization of light and entanglement, they create a secure connection to exchange encrypted keys that can be used for secure communication.

- Quantum processing devices:

These are devices that allow quantum operations to be performed on qubits. They can be qubits that are connected to each other by creating protected cores, or they can be more sophisticated systems that provide enhanced processing capabilities.

- Quantum cloud services (quantic cloud):

Companies that provide cloud access services for quantum computers are another element of the infrastructure. Their services provide high-level access to quantum computer devices and securely distribute data.

- Quantum algorithms:

The development of algorithms adapted for quantum computers allows the use of the power of quantum computers to solve certain problems more efficiently compared to classic computers.

These are some of the essential elements of the infrastructure for quantum technology, but further development in this field will bring new changes and additions in the future.

Features of the transmission environment for quantum technology.

The transmission environment for quantum technology is important, as it must provide adaptability, distribution efficiency and quantum communication. Some of the main features of the transmission environment for quantum technology are:

- Light diffusion:

For the distribution of protected cores, it is important that light is able to propagate excellently in the environment where the device is installed. Environments with small interruptions and low concentrations of pollutants are ideal for them.

- Thermal stability:

Quantum technology devices must have a stabilized environment temperature. Large temperature fluctuations can negatively affect their performance and can cause information loss.

- Minimization of electromagnetic interference:

Electromagnetic interference can affect the accuracy of the results of quantum operations. Environments that provide isolation and do not allow interference are more preferred.

- Information Overlap:

If the information being transmitted is susceptible to external interference, it is important to have mechanisms to reduce or eliminate information overlap. This may include various information encoding techniques.

- Light Intersection Systems:

If light is used to transmit quantum information, light intersection systems are necessary to allow for stable and direct transmission.

- Security and Privacy:

The transmission environment must guarantee the security and privacy of the data being transmitted, including protection from potential hackers and secure and coded transmission.

These are some of the important features of the transmission environment for quantum technology. Providing a suitable transmission environment is essential for the successful operation of quantum technology devices and protocols.

Transmission environments for quantum and binary technology.

The transmission techniques for quantum technology and binary technology differ significantly. Quantum technology is based on the principles of quantum mechanics and uses quantum nuclei and states to transmit and process information, while binary technology uses systems based on the use of numbers 0 and 1 only, to encode and transmit information. While it is theoretically possible to use the same physical environment for both technologies, in practice, there are significant technical and technological differences.

Some of the main differences are:

- Susceptibility to interference:

Quantum technology is much more susceptible to external interference and environmental interactions compared to binary technology. Therefore, it is necessary to better protect quantum transmissions from external interference.

- Protocol structure:

Protocols for quantum transmission are very different from those for binary transmission. They use mechanisms, management, and nucleis that are not used in binary technology.

- Cost and efficiency:

Quantum technology is still in development and is often more expensive and less efficient than binary technology due to the need for specific equipment and advanced infrastructure.

Although theoretically the same physical environment can be used to transmit data via quantum and binary technologies, in practice their use would require different implementation strategies and specific infrastructure for each.

Transmission environment equipment for quantum technology.

Quantum technology is an advanced scientific field that has great potential in many areas, including the environment. Some devices that have been used or developed to use quantum technology to monitor and study the environment include:

- Quantum sensors:

These are devices that use quantum intent to detect changes in the environment. They have higher sensitivity and accuracy than traditional ones, enabling better monitoring of changes in air quality, water, and various chemical contents.

- Quantum cryptography:

It is a technology that uses the properties of quantum mechanics to ensure secure communications. It is used to protect sensitive environmental data, ensuring that information collected about the environment cannot be intercepted or altered by third parties.

- Quantum communication:

Quantum communication technologies are used to ensure fast and secure transmissions by collecting and exchanging data in real time, monitoring difficult areas and at difficult times.

- Quantum simulations:

Through them, it is possible to model and predict environmental changes. Solving complex environmental problems, understanding the impacts of climate change or natural processes is possible with the use of quantum computers.

These are some of the potential uses of quantum technology in the field of environment, and there are often efforts to develop and use other technologies that can help protect and monitor the environment through quantum interactions.

Weaknesses of algorithms in the binary system.

Mathematical algorithms built with the binary system face a number of weaknesses or challenges that can limit their performance in some contexts, such as:

- Representation of large numbers:

Although the binary system is suitable for most applications, it can have difficulties in representing high numbers in an efficient way. This leads to loss of precision or the need to use advanced structures to represent numbers.

- Dealing with fixed numbers:

In the binary system, algorithm numbers are defined based on a fixed number of bits. This can lead to loss of precision for numbers defined with many decimal places (point-decimal).

- Rounded number operations:

If we have to work with rounded numbers on a large scale, the binary system may

face challenges in maintaining the precision of the number.

- Memory requirements:

Some complex algorithms may require intensive processing of high numbers, creating the need for large memory capacity to store the numbers between different processing stages.

- Data interpretation performance:

In some cases, interpreting data expressed in the binary system can be slower than interpreting data expressed in other number systems.

- Implementation cost:

Implementing algorithms in binary can be cost-effective in some cases, but in other cases, it may be more advantageous to use another number system due to the specific needs of the application.

These weaknesses or challenges can be analyzed in some contexts, especially in cases where it is necessary to process large numbers accurately or work with rounded numbers and high efficiency is required. For these algorithms, other number systems can be used, such as the quantum system or finite number systems, which are more suitable.

According to algorithms in binary, to find a particular item among N objects, according to the classical method, it is required to check the entire number of items from 0 to N times. In 1996, Lov Grover1 invented a quantum search algorithm. With his algorithm, a quantum computer only needs to search a number of items from 0 to $\sqrt{N}$ times. With the construction of a quantum computer, this could be used to radically speed up exhaustive key search, while much of conventional cryptography would fall apart.

7. Disadvantages of Quantum Security

Quantum security is a field full of potential, but there are also some challenges and disadvantages that need to be considered:

- Complex infrastructure:

The implementation of quantum security requires special and complex infrastructure, including specific devices such as quantum cores or cells, as well as secure communication channels. This creates difficulties and costs for institutions, organizations and companies in its implementation.

- High cost:

The equipment and technologies required for quantum security are often expensive to purchase, implement and maintain. This can make their use unacceptable for many users of these applications.

- Susceptibility to interference:

Quantum technologies are very sensitive to external interference and environmental

interactions. This can make systems more vulnerable to attacks and gains from third parties.

- Lack of stability and robustness:

Since these technologies are still in the development phase, they may have stability and robustness issues. Therefore, their implementation may be more applicable in critical applications.

- Benefiting from developments in technology:

As quantum technologies are still in development, there is a possibility that attackers will take advantage of them to find ways and means to break quantum security. Thus, challenges to keep quantum systems secure and up-to-date are present.

- Standards and interoperability:

To use quantum technologies efficiently, it is necessary to create common standards and for them to be interoperable with each other. These constitute another challenge of this still developing field and with many different actors in the market.

Vulnerability of quantum security to interference.

Quantum security is prepared to face the challenges of interference, but it is not exempt from insensitivity. There are several factors that can make this security less effective against interference:

- Physical environment:

Interactions with the physical environment can affect quantum devices and protocols. External factors such as radiation, magnetic fields, and different temperatures can cause quantum cores to break or change, compromising the security of transmissions.

- Attacks from insiders:

In theory, intentional attacks by network users or administrators, including physical attacks and the use of fast technological interventions, could affect quantum security.

- Human interference:

Human actions such as physical attacks on quantum infrastructure or attempts to alter or intercept information during quantum transmissions compromise security.

Quantum security breaches.

There are several elements that can compromise quantum security:

- Money scanning techniques:

Techniques used for money scanning can be applied to capture or alter information transmitted over quantum channels. For example, an attacker could use a scanning technique to capture a quantum core and read or alter the data transmitted through it.

- Attacks from within the quantum system:

Deliberate attacks, carried out by parties with legitimate access to the quantum system, can affect the security of transmissions. A system administrator could maliciously

interfere with quantum devices to manipulate data or cause a transmission to be disrupted.

- Attacks from classic computers:

Classic computers can also be used to carry out attacks against quantum security. Through them, a hacker could circumvent quantum protocols and request a private key from a protected quantum core.

- Complete quantum non-communication:

In some cases, complete non-communication between parts of a quantum system can knowingly or unknowingly create low security. When complete non-communication between parts occurs, it can allow an attacker to capture information in an unwanted and harmful way.

These are some of the basic elements that can compromise quantum security. It is important that developers and operators of quantum systems take the necessary measures to cope with potential risks and to ensure their stability and security.

Quantum technology uses various mechanisms to minimize the effects of interference and to guarantee security. We can mention quantum protocols that use quantum distribution of protected cores to ensure the stability and security of transmissions. Most possible attacks on quantum systems require deep technical knowledge and considerable resources, making them more difficult to carry out. However, it is important to understand that although quantum technology offers advanced security, it is not invincible to any type of interference or attack.

Quantum security breach by classic devices.

Despite the high level of security that quantum security offers, it can be breached by classic devices in some cases. This can happen due to several factors that affect the integrity and security of quantum transmissions:

- Classic devices such as electronic and electromagnetic ones can cause interference in quantum devices and processes, which can lead to data loss, unexpected changes in transmissions, or damage to quantum devices.
- Physical attacks using strong classical electromagnetic means against quantum devices can affect the security of quantum transmissions by damaging quantum devices or altering the data that is being transmitted.
- Individuals with access to networks from classic devices, but who also have access to quantum devices, can exploit them to manipulate data or create weak security in transmissions.
- In some quantum systems, complete lack of communication between classic and quantum devices can lead to weak or low security, opening the way for various attacks or data manipulation.

However, unlike classic technologies, quantum technologies are designed to cope with and minimize the effects of these risks. Advanced security techniques can be

used in the implementation of quantum protocols to protect quantum transmissions from interference and potential attacks.

However, it is important that developers and operators of quantum systems are aware of these risks and take the necessary measures to cope with them.

8. Why Quantum Security is Needed, Validity and some Recommendations

Quantum security is important because of what it offers and enables, among which we can highlight:

- Data security:

Quantum technologies offer high levels of security for the transmission of information. The use of quantum concepts such as the distribution of protected and encrypted quantum cores provides a secure way to transmit and receive data, resisting attacks and information capture by third parties.

- Communications security:

Quantum security enables information transmissions to be secure and indecipherable by third parties. This is especially important for communications containing sensitive information, such as personal, financial, or other data.

- Protecting critical infrastructure:

Quantum technologies can be used to protect critical infrastructure, such as financial systems, telecommunications systems, and national security systems, from cyber and other attacks.

- Secure use of quantum computers:

Quantum computers are designed to perform fast and advanced calculations, but they are also susceptible to cyber attacks, making the information and calculations performed on these computers safe and secure.

- Security in telecommunications:

Quantum devices and protocols can be used to achieve secure data transmissions in telecommunications networks, ensuring that communications mediated through them are indecipherable by third parties.

Quantum security is critical to many aspects of modern technology and society in general. Its use can help protect data and critical infrastructure from various attacks and risks.

The value of quantum security compared to financial costs.

The assessment of the ratio of financial costs to what quantum security offers depends on many factors, including the context of use, the level of security required, and the financial capabilities of the organization, institution, or individual.

In certain circumstances, investing in quantum security may be more profitable and justifiable due to the advances in security it offers. Some arguments why quantum security may be valuable are:

- It offers a high level of security for information transmissions. If sensitive or critical data must be protected with special care, investing in quantum security may be reasonable.
- In some areas such as finance, health, and national security, there are laws and regulations that require high levels of security for data and information. In these cases, investment in such technologies may be necessary to meet these legal requirements.
- If the institution, organization or individual is exposed to high cyber risks, investing in advanced security can be an important step to protect its data and infrastructure from third-party attacks and exploitation.

However, in some cases, investing in quantum security may be expensive and not justifiable in relation to the risks and needs of the organization or institution. It is important to make a careful assessment of the costs and benefits before deciding to invest in quantum security. In many cases, the use of quantum security technologies can be an important solution to protect data and infrastructure from increased cyber risks, but a detailed cost-benefit analysis should be considered before a final decision is made.

Some recommendations for legal, protocol and regulatory changes for quantum security.

In general, to promote and increase quantum security, some recommendations for legal, protocol and regulatory changes can be given, here are some of them:

- Standardization and certification:

The creation of clear standards and certification processes for quantum devices and protocols can help ensure the appropriate level of security and facilitate the use of quantum technologies. Institutionally, protocols and processes should be developed to assess and certify quantum devices, protocols and their security.

- Oversight and enforcement:

It is important to have oversight and enforcement mechanisms in place to ensure that organizations, institutions and individuals using quantum technologies comply with security standards and regulations. This includes inspections, incident reporting and disciplinary action for those who do not comply with security standards.

- Establishing policies and procedures:

Organizations and institutions should develop clear policies and procedures for the use and management of quantum technologies to ensure that they operate safely and effectively. These policies and procedures may include rules on access, data protection and training for personnel.

- International cooperation:

International cooperation is important to address the challenges and risks of quantum security at a global level. International organizations, such as the International

Organization for Standardization (ISO) and Interpol, can play a key role in coordinating efforts to promote quantum security at the international level.

- Investment in research and development:

To develop new and innovative technologies for data and infrastructure protection, it is necessary to invest in research and development for quantum technologies, including quantum security. Governments, private industry, and academic institutions can collaborate to finance and conduct research and development in this area.

Conclusions

In conclusion, complex and innovative quantum technology, as a strong clash with classic technology and financial cost, can become a strong mediator for the security of data, information and its transmission, as well as critical infrastructure. It is a tool that offers researchers and developers the opportunity to find tools, facts, and evidence to validate quantum theories related to security. On the other hand, the advancement of this technology can help create vital devices for achieving even more complex goals. In this way, it is possible to accept the mutual co-communication between science and the laws of physics with quantum technology, in their ability to support each other's development.

It is important to emphasize that the effective integration of quantum technology in data security, communication, information, distribution and exploitation should not be simply about using the latest equipment, but also about using quantum technology as a tool to improve the preparation of individuals for the challenges and the creation of intellectual capacities and modern users. We believe that this development will not stop, science promises a lot for the future, just as today artificial intelligence, i.e., expert systems that develop a dialogue with the user, is now a fact.

Bibliography:

1. Daniel Gottesman & Hoi-Kwong Lo "From Quantum Cheating to Quantum Security"
2. J. Preskill, "Battling Decoherence: The Fault-Tolerant Quantum Computer"
3. B. Schneier, Applied Cryptography (2nd ed., Wiley, New York, 1996)
4. L. K. Grover, "In Proc. of the 28th Annual ACM Symposium on the Theory of Computing (STOC), (ACM Press, New York, 1996).
5. E. Biham, "In Proc. of the 31st Annual ACM Symposium on Theory of Computing" (STOC) (ACM Press, New York, 2000).
6. https://www.binarysecurity.no/
7. https://www.paconsulting.com/insights/what-is-quantum-technology
8. http://www.physicstoday.org/pt/vol-53/iss-11/p22.html c 2000
9. http://www.odci.gov/csi/books/venona/preface.htm

The use of tactical drones, tasks and tactics, techniques, procedures (TTP), and their role in the Russian - Ukrainian conflict

Lieutenant Colonel Msc. Eduart PLLAHA
Staff Officer for Air Operations and Reconnaissance
Deplorable Air Command and Control Center (DACCC), Italy

Introduction

With the unprecedented attack of the Russian Federation toward the Republic of Ukraine in 2022 one of the many new weapons that were and are being widely used are Unmanned Aerial Vehicles (UAVs). Ukraine began using tactical drones[1] for reconnaissance in 2014 following the start of conflict in the east of the country with the so-called Donetsk Republic. Ukraine military leaders sought alternative ways to challenge Russia's quantitative and technological superiority in the combat zone by studying the use of UAVs during conflicts in Iraq[2], the Armenia and Azerbaijan conflict for Nagorno Karabakh[3], Libya, Syria[4], as well as against terrorism by the USA, UK, France and Turkey[5] and by Russian special forces when dropping thermite grenades from quadcopters destroyed a series of Ukrainian ammunitions dumps. Tactical Drones (TD) were used from mid-2022 to attack Russian resources and forces, but also for other tasks.

[1] JPCC, "In 2009 the NATO Joint Capabilities Group agreed to divide UAS into three categories, CLASS I, II, and III. Each class is further divided into subcategories with their associated parameters. Parameters such as altitude and mission radius are guidelines, whereas UAV weight is the single determining factor..." and STANAG 4671

[2] J. Parkinson, "Force Protection Consideration" JAPCC, p. 239

[3] Washington Post, "Azerbaijan's drones owned the battlefield in Nagorno-Karabakh" December, 2020.

[4] O. Aksu, "A Methodology for Countering Unmanned Aircraft Systems" JAPCC, p. 133

[5] J. Rogers, "Future Threats: Military UAS, Terrorist Drones, and the Dangers of the Second Drone Age", 2021, JAPCC

These air vehicles provide the Ukrainians with 86 percent of all targets, and from 2023 to the summer of 2024 they are credited with the destruction of about 2/3 of the Russian tanks in Ukraine or about 1550 pieces[6], having an indisputable impact on the battlefield. The use of TDs on both sides has made the battlefield almost transparent providing adversaries a view of almost every object or action of one another; from troop concentrations in depth to front line trenches.

First-Person-View (FPV) drones with onboard ammunition have become more effective thanks to the ability to hit individual vehicles or even groups of targets with incredible precision and cost-effectiveness[7]. TDs have achieved "precision" superior to artillery in this conflict because they can change course to hit targets in movement, in shelter, or in fortification focusing on weak points such as optical and sighting tools, engine etc. These assets have achieved freedom of movement in low-altitude "air littoral"[8] at low-intensity conflict, without the need for combat aviation and, together with artillery, have brought about a frontal, static and trench conflict like that of World War I.

As a result of several decisive factors such as the development of "smart" technologies, 3D printers and the electronic control system these air vehicles have become multi-role, very usable and quite efficient[9] on the battlefield. Above all, the possibility to produce and assemble them without the need for production-assembly lines of large enterprises, but through small initiatives (start-up) in improvised environments or in garages by volunteers[10].

In this paper we will first focus on the role and importance of drones in the war in Ukraine, since according to many analyzes of conflict researchers, drones have revolutionized modern warfare and has changed character of the war[11]. Second, we will look at the components and munitions they use, as well as some drones successfully used by both sides in the conflict. Third, we will explain the organization of the drone units and the training of the operators. We will then see some of the tasks and ways of use at the tactical level. In conclusion, we will give some suggestions for Albanian Armed Forces along with the approach towards them, that some NATO member countries have and those in the Balkan region.

---

[6] J. Detsch, "Ukraine's Cheap Drones Are Decimating Russia's Tanks but experts say they're not a long-term solution to a lack of artillery rounds" Foreign Policy Magazine, April 2024

[7] F. W. Kagan, K. Kagan, M. Clark, K. Hird, N. Bugayova, K. Stepanenko, R. Bailey, G. Barros "Ukraine and the Problem of Restoring Maneuver in Contemporary War", ISW, Aug, USA. 2024, p. 11

[8] M. K. Bremer, K. A. Grieco, "Airpower after Ukraine, Air denial: The dangerous illusion of decisive air superiority," Atlantic Council, 2022

[9] M. L. Khan, "The Crowdfunded Drone War in Ukraine", National Inters, 25.08.2022 "*they become robust, efficient, small, and affordable enough to be used by a broad range of operators for a variety of tasks*"

[10] Ch. Mamo, "Revitalizing Ukraine's Defense Sector, and with It, Its Military" Emerging Europe, 2021

[11] ISW, "Ukraine and the Problem of Restoring Maneuver in Contemporary War", USA. Aug, 2024, p. 24

1. Tactical drones, their components and method of manner

The drones we will focus on in this article are classified by NATO as "Class I" weighing less than 150 kg. They are categorized as "mini" and "small", and used by tactical units (squad to battalion/regiment)[12] with and operating altitude of up to 1500m (5000 feet) and operational range is up to 50 km (this operating range is used by the unit's that are operating them at the tactical and operational level). Drones of this class are also considered Tactical Drones (TD) for the tasks they perform in support of tactical units and we will refer to them in this way. Their notation is more historical than specific as there are no clear boundaries of definition[13] and the terms of use are often interchangeable between them. They can be used for "one-way attack" also known as kamikaze or suicide drones and "multi-use" also known for reconnaissance, bombing, data relay and electronic warfare etc. In terms of lethal effects mini and small drones discussed in this article stand out: First-Person-View (FPV), One-Way-Attack (OWA), and loitering munitions[14]. Flight control of these TDs are also marked as FPV[15]/ Video Piloting drone, a method used to control a UAV from the pilot's viewpoint. Their course is carried out directly by the operator, through an onboard camera providing a video feed to FPV goggles or a monitor. The pilot directs, reacts and corrects the flight path through the commands given by the control handle as he has a view directly on the screen of the glasses (pic 1). This feature provides a "pseudo pilot's eye"[16] on the drone to direct it as if the pilot were on board. This method provides reaction time to avoid obstacles, terrain, and consumes less on-board battery. The image provided by the camera can be viewed as a live video on tablets, mobile phones and monitors in operational or management centers. The difference from other so-called Kamikaze and Loitering drones, is that these FPVs are commercial drones, and are modified by attaching ammunition on them. Kamikaze drones are mainly manufactured for this task and the munitions are installed on board in production lines, such are for example

Pic. 1: First Person View "*Ukrainska Pravda*"

[12] NATO fixed-wing UAS Classification (AEP-4671) and "Group 1" according (DoD)

[13] D. Hambling, "Ukraine's Mysterious New "Rocket Drone" Will Target Russian Air Force" Forbes, 28.08.2024

[14] D. Kunertova "Drones have boots: Learning from Russia's war in Ukraine", Contemporary Security Policy, p. 582.

[15] UK Civil Aviation Authority, "Drones fitted with video cameras often provide an opportunity to downlink live video to the remote pilot either via a mobile phone, tablet computer or other screen, or even through video goggles - this capability provides the pilot with a pseudo pilots eye view from the drone is generally known First Person View"

[16] Ibid

Lancet, Zala, Shahed, Switchblade which we will see below. TDs can be multi-rotor or fixed-wing. Multi-rotor drones are mostly small UAVs with the ability to stay in the air flying over the same point (hovering) and less expensive, such as DJ Mavric. Fixed-wing drones are larger with more on-board equipment and expanded carrying capacity. They use aerodynamics for lift, which is produced by its body and wings, e.g. Ram II. Some TDs may also have specialized equipment such as Sensor Turrets with infrared sensors, laser designator and electro-optical cameras, navigation (GPS) and autopilot to return to the base, etc.

The body[17] of the FPV is built with carbon fiber, plastic or wood and the frame can be shaped in the form of "X" (pic. 2), "H" and square. Their propellers usually have a diameter of 18cm, while bomber drones use two blade propellers with a diameter of 10cm. A video transmitter, radio signal receiver for control from the operator's control handle, the battery, sensors, as well as the ammunition holding device and the ammunition are mounted on the body. The computer unit is center-mounted and connected to an analog or digital camera. The main parts of the FPV are produced by 3D printers using a plastic material and takes several hours to produce from the production of components to manually assembly by workers.

Part of the operation set is the control handle which directs the UAVs housing the receiver-transmitter module and joystick control. The control handle also provides the ability to change the flying frequencies. Goggles include a video-receiving module and antenna. Operators of these TDs can fly them from a vehicle equipped with receiving equipment, generally consisting of an analog video receiver matching the frequency of the TD transmitter and a viewing device, from the operational center, or from the ground. To achieve greater control range and increase the operating distance, high-gain antennas and amplifiers are sited but also on another UAV. These antennas and amplifiers can be placed close to the frontlines and away from the operators' site. This provides increased video clarity and range of the operation. Also, protection of UAV from the Electronic Attack and the operators can operate them from defenses and shelters.

The control of FPVs is maintained through two radio-links, the first for transmitting the aerial view to the control unit, which allows the operator to fly it to the target in

[17] J. L. Parker, "Mission Requirements and Aircraft Sizing", at: "Special Course on Fundamentals of Fighter Aircraft Design", NATO Advisory Group for Aerospace Research and Development, AGARD Report No. 740, 1987, p. 2-16.

order to accomplish the task, and the second for sending command signals from handle to the drone. The video that is transmitted from camera to the command unit can be digital or analog according to the camera. The FVP operator can lose communication with the drone when operating frequencies are targeted for suppression by Electronic Warfare resulting in disruption of digital video or excessive noise for analog video. The majority of Ukrainian drones still operate on range of 850-930 MHz[18] making this frequency range the most targeted by Russian Electronic Warfare (EW) seeking to suppress it. At the same time, Russian kamikaze drones use communication modules with alternative reception and transmission frequencies in the range of 720-950 MHz or 950-1100 MHz. The 900 MHz frequency provides a long range of FPVs even in wooded areas, vegetation, and buildings but requires relatively large antennas. While 5.8 GHz has gained popularity in recent years as its equipment is very cheap and the antennas are relatively small and offer good video views combined with driving glasses, but it has a weak signal in environments with dense objects and vegetation, in water environments or even concrete constructions[19]. Each frequency has different features and characteristics which by interconnecting and with additional equipment such as larger transmitting antennas and located at high-gain can reach up to 20-30 miles distance. Radio frequencies for FVPs are effective within line of sight (LOS), moreover, they require amplifiers and larger transmitting antennas or repeaters. These last ones increase protection against EW and amplifier boosts the communication frequency. Some UAVs can have alternative reception and transmission frequencies making them invulnerable to EW systems because they can operate on different frequencies.

- **Tactical Drone Munitions.**

Tactical attack drones with explosives on-board, modified and produced in local workshops were first used by ISIS units in Syria[20], and to attack a tank with ammunition on-board by ISIS in Iraq[21]. In Ukraine, the PG-7 (85mm) anti-tank grenade was widely used for attack FPVs (Pic 2). This projectile is used by RPG-7 launchers and offers armor penetration of up to 260mm of steel. Russia's most advanced tank, the T-90, has 500mm of blend of steel at the front but at the rear hull/ turret is less than 40mm providing a weakness easily exploited by FPV operators resulting in the destruction of a tank which cost around 5 million dollars by a 400 dollar FPV drone. Quadcopters like "DJI Mavics" and "Baba Yaga" are usually armed with modified grenades designed for use against infantry. Initially, these modified hand grenades, corresponding to Vog-17 (30mm) and M-433 (40mm) from an automatic grenade launcher AGS-17 and M-203/320 (40mm) grenade launcher, came from the Soviet Union, USA or German, etc. Besides these munitions, attack drones can be armed

[18] Yann, "How Is the Drone War Evolving, and Why Is Ukraine Lagging Behind in It?", at MILITARNYI, 20 Feb, 2024.

[19] First-person view (radio control); https://en.wikipedia.org/wiki/First-person_view_(radio_control)

[20] O. Aksu, "A Methodology for Countering Unmanned Aircraft Systems", JAPCC, p. 133

[21] J. Parkinson, "Force Protection Consideration", JAPCC, p. 239

with improvised explosive devices (IEDs) produced in home, terrain, foundry, etc. These IEDs consist of soda cans and 3D printed plastic as a body filled with plastic explosives or TNT obtained from artillery shells. Fusing is done using a hand grenade fuse, impact fuse, or electric fuse. These munitions are produced by Ukrainian state-owned enterprises and private start-ups which have shown efficiency and quick adaptation to requirements. From a financial standpoint, these munitions are several times cheaper than, for example, 155mm artillery shells which costs around 2-3000 dollars. To increase attack accuracy of the unguided munitions, these bombs have also been fitted with plastic wings. Also, they are well balanced and can be carried without affecting the flight course of the drone enroute or during the attack on the target. Part of the ammunition arsenal of these drones are 82mm mortar shells and anti-tank mines. OWA drones can be equipped with munitions designed for fragmentation, anti-tank, incendiary like the Molotov cocktail[22], or dual-purpose (anti-personnel and anti-armored) (pic 3).

Pic. 3. The range of munitions ...fragmentation, anti-armor & duel-purpose bombs of various sizes ... [+] Steel Hornets

- **Tactical Drones used in Ukraine.**

During the Russia-Ukraine conflict, many types and models of tactical UAVs have been used, below we will see the longest range models. Ukraine has a large number of TDs and by June 2023 had accepted around nine models[23] of OWA drones including six FPV quadcopters and three fixed-wing versions. This is a result of the rapid change in the technologies, the support of various western countries, and domestic production[24].

Fixed-wing UAVs can fly at short and long ranges, as well as at low and medium altitudes for operational and tactical tasks. They can be used for OWA, target acquisition, precision strike capabilities as well as ISR. These UAVs are very effective for long-distance flights and weight bearing, but they do not have high maneuverability, and require landing and takeoff conditions such as platforms, runways, etc. They are also more protected against EW systems used by front-line tactical units as they fly relatively high and the domes created by them are less effective. We will start this category with the "Punisher"[25] model produced in Ukraine. This model had very good characteristics and were used during the first stages of the conflict for

[22] D. Hambling, "Steel Hornets: Inside Ukraine's Amazon for Drone Bombs", Forbes, 2024

[23] Ukrainian Military Portal, "FPV drones: weapons that changed the modern war", 2023

[24] Ch. Mamo, "Revitalizing Ukraine's Defense Sector, and with It, Its Military,", Emerging Europe, 2021

[25] A. Lowther, M. K. Siddiki, "Unmanned aircraft systems Combat Drones in Ukraine", Air Space Operations Review 3

reconnaissance, attack, etc. This UAV weighs 2 kg, and has an operating range of 45 km, wingspan of 2.3m, and autonomy of flight around 90 minutes and with altitude up to 400 m. The second example is the Polish-made "Warmate"[26] that was used for the same tasks, weighs 5.3 kg, operating at up to 150 km/h with 70 minutes autonomy of flight, with an ammunition payload of around 1.4 kg. Also, this drone can be controlled manually by an operator and through a programmed automatic control. Also in this category are the US-produced OWA "Switchblade 300/600" drones. They have a manual and autonomous control systems and have been against fortifications and high-value assets such as repeater antennas, electronic warfare equipment, etc. The "600" variant has a larger ammunition payload[27] and has been mainly used against tanks. The "300/600" models weigh 2.5/15kg, and measure 49/130cm in length with a wingspan of 76/150mm wingspan. Their operational range is 10/40km with an autonomy 15/40 minutes, as well as a flight altitude below 150m and a speed of 101/113km. As for the single-use TD with fixed wings and long range, we will see the "Ram II" model, which is launched using a special catapult which can be installed on an armored vehicle or SUV. The Ram II (pic. 4) is a high-precision drone with an operational radius of 30 km, a speed of 70 km/h, autonomy of 55 minutes[28], and maximum altitude of 1,000 meters. Its maximum take-off weight is 9.8 kg, with a 3 kg payload capacity and measuring 10 m in length with a 2.5 m wingspan. The RAM II is primarily used to attack valuable equipment such as anti-aircraft systems using a thermobaric, High Explosive Anti-Tank (HEAT) warhead or HEAT Explosive/Fragmentation warhead, which is designed to destroy open personnel targets. The RAM II targeting uses an active visual target tracking system to lock on a target using live video from onboard camera allowing the RAM II to track a target with the aim of knocking it out[29].

Pic. 4:Illustrative photo from: *Militarnyi.com*

Rotary wing drones are highly maneuverable over complex terrain as they can make quick turns, hover, take off and land vertically. They can perform non-kinetic tasks such as providing situational awareness, conducting reconnaissance, providing target acquisition, correcting artillery fire, or kinetic tasks such as attack and bombing. The main drone in this category is the "DJI Mavric" which is a Chinese product and was originally used by volunteers and territorial forces. This drone has several models

[26] Ibid.

[27] AeroVironment Switchblade, https://en.wikipedia.org/wiki/AeroVironment_Switchblade

[28] S. Tiwari, "Ukraine Showcases Its Indigenously-Built RAM II Loitering Munition at IDEX 2023, Close to The Russian Stall", The EurAsian Times, 2023

[29] Ibid.

with different characteristics, mainly in terms of autonomy of flight, camera resolution, availability of thermal cameras, etc. The most successful model has been the "DJI Mavric 3" which has an operating range of 12 km, autonomy of flight 41 minutes, weighs 960gr., operational altitude of up to 6000m[30], at 54 km/hour and controlled via 4G mobile. Its camera offers very good viewing angles up to perpendicular in reference to the ground. This drone is used for reconnaissance and attack missions using mounted munitions with great creativity and versatility. The Mavric 3 continues to be one of the most important in this conflict and is also used by Russia. Among the most famous and successful bombers for the "quadcopter" class is the Ukrainian-made "Baba Yaga" drone. It continues to be used as a relatively large bomber compared to the DJI Mavics. Its payload is several kilograms and is usually armed with modified grenades, up to six 82mm mortar shells or 10 kg anti-tank mines which have been used stop attacks by armored vehicles or to block corridors opened by the Russians towards the Ukrainians. Also, "Baba Yaga" has a high-precision attack calculation system and is mainly used for night flying as it has thermal cameras, can operate in difficult flight conditions and is very resistant to EW attacks due to the satellite communication terminals on board. One of the main Ukrainian models of OWA FPV (quadcopter) is "Pegasus" (pic. 5) which the Ukrainian volunteer group Escadrone produces at a rate of almost 1000 pieces per month. This drone takes about 5 minutes to set up and take off, but requires great skill to maneuver on the battlefield. The Pegasus drone has a top speed of 70 km/h, and can stay in the air for about 10 minutes. Each Pegasus costs around 400 euros and most of the parts are produced by 3D printers. It is produced in two variants, respectively with an ammunition payload of 1 and 2 kg. The KH-S7FPV (quadcopter) can be used to attack mobile and fixed ground targets with an up to 1 kg payload and max range of 9.5 km. Its camera produces good quality of video and can also be used for reconnaissance.

Pic. 5:Illustrative photo from: *Militarnyi.com*

Russia, was one of the leading countries in the world for production of military hardware during the first year of the conflict, but did not show modern and aggressive use of tactical UAVs on the battlefield, choosing instead to stick strictly to its doctrine which used UAS for ISR, direction of artillery fire and EW. Despite focusing on these areas UAS employment was not fully accomplished successfully likely due to the fact that Russian UAS (of different categories) were not among the most advanced in the world[31], even after the conflict in Syria showed a special importance both in

[30] BBC, "How are kamikaze drones being used by Russia and Ukraine?", 29 December 2023

[31] S. Bendett, "Where Are Russia's Drones?" Defense One, 2022, https://www.defenseone.com/

terms of diversity and their integration at almost all levels. At the start of the conflict, Russian UAS employment was far behind Ukraine, tactically and operationally, and this began to change in the spring of 2023 before the start of the Ukrainian offensive, when Russia shifted to UAS use extensively for attack, correction of artillery fire, data relay, etc. At this point, Russia decentralized[32] the decision-making to attack targets in the charge of local commanders or drone operators, unlike the beginning which was centralized in the command post of large ground units and was taken by the unit commander. Subsequently, Russia began importing drones from Iran and began produced them in Russia but with difficulties and problems as it is under the effect of the embargo on the main parts of UAVs and electronic chips.

We are starting with fixed-wing drones that take off through a catapult, and the most successful in this category for Russia is the "Orlan-10"[33], a medium-range, multi-purpose tactical drone. This UAV is usually used for recon in support of artillery to detect targets and transmit their coordinates to artillerymen, as well as counterbattery fire. It is cheap and simple to operate, good performance, and its resistance to jamming[34]. This UAV has composite fuselage and can fly day and night. The Orlan-10 has modular design which provides for several interchangeable payloads to include EW, attacking electromagnetic spectrum used by the adversary[35] through mounting interference transmitters and suppress mobile communications as part of the Leer-3 electronic warfare complex. Video and imagery used for reconnaissance are transmitted to the ground control in real-time through a data link using 3G/4G cellular networks. These UAVs are deployed in groups of three; the first is used for reconnaissance, the second EW and the third as a data relay. The maximum take-off weight is 15 kg with a 6kg payload, maximum speed of 150 km/hour, combat radius up to 110 km, a 16 hour endurance and service ceiling up to 5000 m. Another successful fixed-wing drone which is launched via catapult is the Lancet-3M that can be used for both reconnaissance and strike missions. This UAV has body designed like the letter "X" and it can fly day and night. It weighs 12 kg, has a speed of 112 km/h and maximum range of 40 km. This drone can be armed with high explosive (HE), HE-fragmentation or shaped charge warheads from 2 to 6 kg and is mainly used against important objects such as air defence systems[36], artillery, tanks, etc. Launcet-3M uses optical-electronic guidance and a TV guidance unit[37] for controlling by UAV operator.

---

[32] J. Bronk, N. Reynolds, J. Watling, "Ukraine and the Problem of Restoring Maneuver in Contemporary War", "*The emergence of a decentralized, drone-based TRSC on the Russian side in roughly May & June 2023 has enabled Russian troops to identify & prosecute targets much more quickly than they had previously been able*" p. 10

[33] Ibid, p.16

[34] Ibid, p.20

[35] B. Nikolov, "Russia produces about 167 FPV drones per hour, says Moscow", Forbes, 01,08,2024

[36] ORYX Blog, "Attack on Europe: Documenting Ukrainian Equipment Losses During the Russian Invasion of Ukraine".

[37] B. Justin; W. Jack, "Mass Precision Strike: Designing UAV Complexes for Land Forces", RUSI, p. 26-27.

As for FPV drones, Russia has mainly has been supported by volunteers who produced and assembled parts on commercial UAVs to turn them into "one-way attack" or for other tasks. These TDs are known as weak production and sensitive to EW[38]. They were accepted for battlefield use and integrated gradually with favorable reception by Russian commanders after they observed Ukrainian success with similar assets. The main model is the "VT-40 FPV" quadcopter which is produced by the Sudoplatov volunteer group under the contract of the MoD with a production rate up to 1000 per day[39]. It has a payload of up to 3kg and flies at a range of approximately 10km. The VT-40 FPV mainly suffers from problems in its control frequencies from the ground. Another successful quadcopter model for the Russians is the Ghoul FPV armed with RPG-7 warhead which is developed and produced by the volunteer group with same name.

3. Training of Operators and the structure of Tactical Drone units

The importance of dedicated training centers for drone operators has been fully confirmed in recent conflicts such as "Second Nagorno-Karabakh War" in 2021. In this conflict, the role of the center opened by Azerbaijan in 2018 with the aim of increasing their combat readiness, competent and efficient use of UAVs in various tactical and meteorological conditions came out clearly. Also, Azerbaijan has established the Drone Academy in order to increase theoretical and operational skills. The same thing happened with Ukraine, which has opened several drone operator training schools since 2014, first to prepare them for reconnaissance tasks, then, following the start of the conflict with others tasks such as bombing, attacks with OWA drones, etc. Ukraine trains drone operators for 33 days[40] in which 20 hours are spent using a simulator with the remaining time spent on practice with actual drones. Computer programs help operators fly FPVs successfully even in the most difficult tasks by integrating Artificial Intelligence. Artificial Intelligence is used to perform most of the task with operator intervention when important decisions need to made such as attacking the target. First, the operator switches the UAV to operate autonomously after identifying the target before programing the drone to continue the attack even when the target is in motion. Drones can follow a pre-planned flight course if it is attacked by EW[41]. This course can be to return to base or to continue flying until the electronic attack concludes or is repelled when it is to resume duty. Seeing the effectiveness and the role that these FPVs play in this conflict, Russia also started to open training centers and academies preparing around 3500 operators[42] in 2023. The Russian course lasts 1 month and includes exercises in the simulator and practice.

[38] D. Hambling, "Ukraine's Kursk Offensive Blitzed Russia with Electronic Warfare and Drones", Forbes, 2024

[39] D. Hambling, "Russian Volunteer Group Claims to Make 1,000 FPV Kamikaze Drones a Day" Forbes, 05.12.2023.

[40] D. Hambling, "New Software Makes Everyone an Ace FPV Pilot", Forbes, 20. 02. 2024

[41] Ibid.

[42] B. Nikolov, "Russia produces about 167 FPV drones per hour, says Moscow", Forbes, 2024

While the training varies depending on the type of UAV the cause includes building, fixing, arming and operating drones through the hatches of vehicles and how to carry out kamikaze attacks.

Usually, the smallest UAV unit is a "group" consisting of three personnel; the commander, the UAV operator and the vehicle driver. UAV groups usually operate from a pickup truck to move and carry about six FPVs[43], transmitting antennas, ammunition and communication radios and other necessary equipment. Each drone is controlled by a single pilot. Usually two groups work in pairs at a distance from each other in order to create redundancy on coverage with radio signal while complicating targeting of their positions. This model offers the optimal use of resources where one group launches UAV and the other does the recovery, repeating this method again and again. It also makes it possible to have different vectors as angles of attack on targets. A platoon consists of four groups and a company with three platoons. Every Ukrainian Brigade has a tactical strike company of drones with around 24 attack drones and the same number of drones for reconnaissance. The UAV battalion[44] may consist of three companies; attack, ISR and support. A battalion could be assigned in support units in the main directions of the front.

4. Main Tasks and Stratification of Tactical Drone to create effect on the Battlefield

In this topic, we will give some tasks tactical drones are executing in the Russia-Ukraine conflict. Starting with the FPV for attack than for reconnaissance and continuing with adjusting and correct artillery fire from the wide range of tasks they can perform. It should be noted that some of these tasks are not dedicated to certain types of drones, for example; the attack FPV while on mission may perform ISR task by transmitting live video from battlefield. Also, long range one-way attack drone during their course of flight, may detect targets and transmit their coordinates to artillerymen to attack the detected targets or by other drones of same category.

The Armed Forces of Ukraine are using TDs for attack, mainly FPV drones to attack anything that moves in front line and even attack helicopters like (Mi-28, Ka-52) and reconnaissance drones taking tactical victories without endangering the troops. Their combat radius is from a few meters out to approximately 20 km in depth for short-range drones and with autonomy of flight from 10 minutes up to 1 hour. Long-range TDs operate between 15 and 40 km and autonomy of flight of several hours where they are dedicated to attack important assets. The range of action for these drones and the definition of short- and long-range typology is very vague as it depends on the support elements that make the task possible such as the battery, radio wave amplifiers, antennas, as well as the terrain such as mountainous or forested, weather

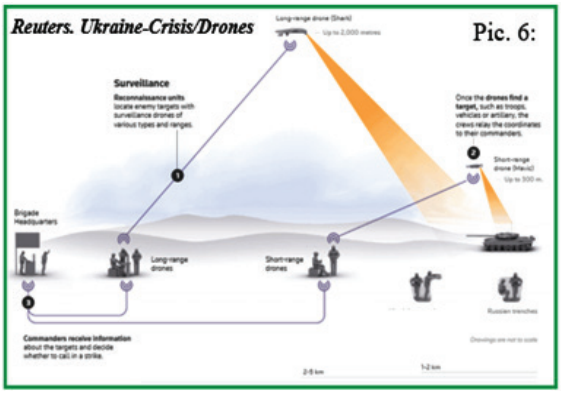
[43] J. Bronk, J. Watling "Mass Precision Strike Designing UAV Complexes for Land Forces", RUSI, 2024, p. 40

[44] Ibid, p. 26

conditions, and from dense of electronic warfare, air defense, etc. Also, the area of action in order to attack the targets depends on the importance of the targets as the operator can attack with long-range TD an air defense system even though it may be positioned several km away from the front. In an effort to protect troops and hardware from drones Russia has invested a lot in EW against UAVs with relative success since the news coming from the front[45] shows drone operators continue to destroy military assets every day, even grenade-armed robotic mini-tanks[46] un experimental unmanned ground vehicle (UGV).

The core mission of *attack* TD/ (FPV) is to degrade the fighting effectiveness of the adversary. The intent is to halt the movement of hostile forces before they can close to within direct-fire weapons range of friendly forces[47]. This can be achieved by destroying significant numbers of adversary capabilities (artillery, armored vehicles, EW systems, maneuver elements, support vehicles, depots, etc.) from the depth of the front line through long-range drones (such as RAM II and Switchblade, Lance 3M). It is worth noting that targets *at a distance of 30-50 km* from front line are mostly outside the range of artillery and short-range TDs, that is, an *operational distance* where the attack against them is usually carried out by aviation. TDs, after reaching the area of operation, start searching for the target through active visual target tracking system using the real image coming from on-board camera. Once a target is located the operator locks on using this system to stay in sync with little or no control from him with the aim of knocking it out.

At a *distance of up to 10 km* from the front line, adversary fighting formations can be attacked with FVP drones such as Pegasus and KH-S7FPV (pic. 6). At this distance the enemy's forces are dependent on armored vehicles to reach the opening point where they will launch an attack. These FPV drones are called after opposition forces have been detected by reconnaissance drones. As we mention above, FPVs do not stay in flight to wait for opposition forces to appear because loiter time is limited. FPV units are mostly positioned at a distance of approximately 500m from each



[45] ORYX Blog, "Attack on Europe: Documenting Ukrainian Equipment Losses During the Russian Invasion of Ukraine"

[46] D. Axe, "The Russians Sent a Platoon of Grenade-Hurling Robotic Mini-Tanks into Battle. The Ukrainians Blew Up the 'Bots in the Usual Way: With Drones", Forbes, 31.03.2024

[47] J. Bronk, J. Watling, "Mass Precision Strike Designing UAV Complexes for Land Forces" RUSI, 2024, p. 26

other to increase redundancy, provide mutual support, as well as to have different angles of attack, etc. A mission requires a large number of drone (depending on the amount of forces) to arrive in a short period of time, to rapidly degrade attacking and supporting formations as they advance to overwhelm point defense. The ammunition used to knock out armored vehicles usually consists of a shaped-charge warhead, for example PG-7. At a *distance of about 2.5 km* from the front line, the offensive TD units interact closely[48] as a unified force with the defensive forces to achieve tactical victory (pic. 6). Defensive forces use their weapons such as anti-tank rockets, grenade launchers, large-caliber machine guns, mortars, etc., with the same mission stopping and degrading human resources, armored vehicles and tanks of opposing forces at the company level.

Short-range TDs for *ISR (Intelligence, Surveillance and Reconnaissance)* can fly from a few hundred meters to about 10 km[49], as well as long-range ones of approximately 50 km from front line and support tactical units with ISR. The autonomy or time of staying on the air starts from a few minutes to a few hours to fulfill tasks. The mission for close ISR is to provide persistent[50] and widespread coverage for units in the close fight. One of the lessons learned in this conflict is that units with uncompetitive situational awareness are liable to suffer disproportionately in engagements[51]. These ISR drones already are part of these tactical units and as we saw above this task can also be performed by attack drones or EW UAVs. Rotary TDs are most efficient for close ISR and can be carried by dismounted personnel. Also, they perform ISR during the day and at night and transmitting live video from the area they are flying over to the operators or unit commands (pic. 6) for the opponent activity. Meanwhile Long-Range TDs are usually fixed-wing and have ability to fly and loiter in depth and with EO/IR sensor payloads to fulfill their task. Endurance, in term of flying to area and identifying targets is one of main key elements of these platforms. Dispersal and density of this UAV at the front is key to the success of units and for this reason their losses are high, e.g. in the city of Bakmut alone, where about 50 Ukrainian drones[52] were flying at any time conducting vital missions in surveillance, intelligence gathering, early warning, and precision strike roles.

TDs can conduct vital missions supporting artillery by *adjusting, correcting and Direction/Aiming artillery fire*. Not only those UAV that are dedicated for supporting artillery like Spectator-M and Leleka-100 but also other UAV during their flight course to the object or the area of operation by improving Artillery Firepower of tactical and operational units. While the TDs have a short-range and flying time and

[48] Ibid, p. 26

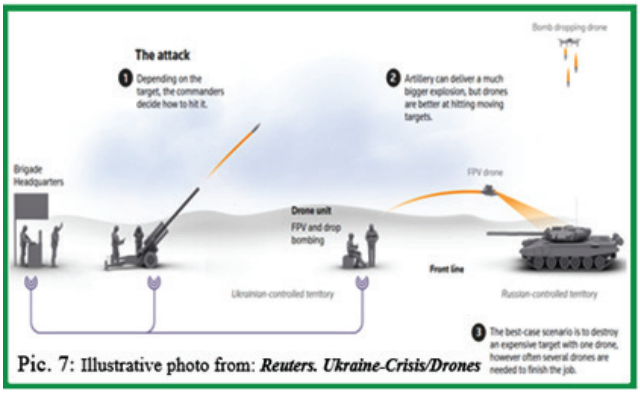
[49] Ibid, p. 22

[50] J. Bronk, J. Watling, "*Author interviews with Armed Forces of Ukraine General Staff, operational groups of force commanders and frontline troops, Ukraine", … 2022, May, July and October 2023, and February 2024*, p. 24

[51] Ibid, p. 24

[52] S. Joshi, "The war in Ukraine shows how technology is changing the battlefield", The Economist, 2023.

ease of availability makes them a practical and expendable option for artillery spotting. During this time, UAVs continue to supply the different unit commanders with aerial images (pic. 7) to take decisions such as attacks with large caliber artillery (155/152 mm), tube artillery (HIMARS), or with aviation, as well as to make an assessment of attacks and its correction. TDs can attack the targets that are DT/ TST (Dynamic Target/Time Sensitive Target)[53] according to the latest assessments carried out at the command in a quick time of up to three minutes[54] through artillery. TDs on the battlefield are tracking and spotting troop movements in real time and providing this information directly to artillery units allowing fire missions to conclude in approximately in three minutes.



Pic. 7: Illustrative photo from: ***Reuters. Ukraine-Crisis/Drones***

These TDs contribute to intelligence mapping software, like Kropyva[55] (Nettle in English) which helps map targets and coordinate artillery fire missions through a NATO compatible secure communication network at all levels (from divisional command to an individual tank), but crucially, is devised to work in cooperation with drones. The live video from the drone reports on where the artillery point of impact allowing the system to suggest adjustments to artillery units until the target is struck. Also, battlefield management systems like GIS Arta, Combat Vision[56] share data, locate targets, and direct fire. According the military experts, the use of TDs to support artillery units has reduced the consumption of rounds; for example, destruction of a standard platoon in a defensive position using artillery typically required about 75 rounds from a 120-mm, but UAV integration has reduced this to just nine rounds[57]. Combining an Automatic Tactical Management System, 'Kropyva', with drones for fire correction has increased the effectiveness of Ukrainian artillery and shortened the time required to deploy a howitzer battery to three minutes, the time required to engage an unplanned target to one minute, and the time required to open counter-battery fire to 30 seconds[58].

[53] Joint Publication 3-09 "Joint Fire Support", 10, 04, 2019, p 78

[54] J. Watling, O. V. Danylyuk, "Preliminary Lessons from Ukraine's Offensive Operations, 2022-23", Rusi, 2024

[55] T. Cooper, 'Kropyva: Ukrainian Artillery Application', Medium, 19 June 2022.

[56] S. Hilton, "How Drone Support is Improving Artillery Firepower The eyes in the sky are reinventing long range weaponry", Polymer Nano Centrum, 2023

[57] A. Molloy, "Drones in Modern Warfare Lessons Learnt from the War in Ukraine" Australian Army Res.Center 2024

[58] Hunder, Zafra, Rao Kiyada,'How drone combat in Ukraine is changing warfare', Reuters, 2024

This class of TDs has allowed Ukrainian units to stop the Russian advance even in the absence of artillery shells, achieving tactical victories on the ground across almost on the entire front. Also, TDs have provided about 86%[59] of the attacked targets from Ukraine Armed Forces. Through TD employment, Ukraine has created *new operational space* (air littoral)[60] and been able to dominate it with drones and loitering munitions during first phase of conflict (2022-2023). Later achieving localized and temporary air superiority[6162] at low altitude/air littoral[63] *at a given time and place,* and through it they are executing tasks that in the traditional concept were mainly performed by aviation of whom has Air Superiority at the front. The contested[64] *air littoral* has emerged as a critical new subdomain of warfare in this conflict. Meanwhile Ukraine does not have air superiority at other altitude levels, also they have had denied of air superiority to Russian air force in the medium and higher altitudes where fighters and bombers typically operate.

5. Tactics, Techniques and Procedures (TTP)[65] of using tactical UAV

In Ukraine we have seen massive use of tactical drones for kinetic and non-kinetic tasks. For the realization of these tasks, we will see below the Tactics, Techniques and Procedures of using these air vehicles. Thanks to the evolution of the counter-UAS systems technology[66] we have a rapid change of TTP. Tactical drones associated with precision rocket artillery, aviation and Electronic Warfare have brought the change of concepts/doctrine and therefore TTP.

Tactics are considerations that dictate how these tactical drones should be used on the battlefield[67]. TD tactics usually provide specific, or general, useful guidance to

[59] D. Kunertova, "Drones have boots: Learning from Russia's war in Ukraine", Contemporary Security Policy, p. 582.

[60] J. Maxa, "Air War over Ukraine: Lessons for Taiwan", Security Outlines, 2023, "However, the dominate was short-lived as Moscow quickly learned how to counter it through mainly EW".

[61] M. K. Bremer, K. A. Grieco, "Airpower after Ukraine, Air denial: The dangerous illusion of decisive air superiority," Atlantic Council, 2022

[62] NATO definition of Air Superiority: '*The degree of dominance in the air battle of one force over another which permits the conduct of operations by the former and its related land, sea, and air forces at a given time and place without prohibitive interference by the opposing force*,'

[63] M. K. Bremer, K. A. Grieco, "The Air Littoral: Another Look," Parameters 51, no. 4 (Winter 2021–22):, p. 68, "*the area from the Coordinating Altitude to the Earth's surface, which must be controlled to support land and maritime operations and can be supported and defended from the air and/or surface"*

[64] Lt. Gen. David Barno, Nora Bensahel, "Drones, the Air Littoral, and the Looming Irrelevance of the U.S. Air Force" War on the Rocks, USA, March 7, 2024.

[65] AFTTP 3-2.3, "Air Force Tactics, Techniques, and Procedures"

[66] O. Molloy, "How are Drones Changing Modern Warfare?" 2024, "*The moment the UAS were used, the counter-UAS systems emerged, and then the tactics, techniques, and procedures (TTPs) had to be adapted, etc. The TTPs that worked for the first six months of the war no longer work today – both the platforms used and the tactics that underline the use of those platforms*"

[67] This paraphrase is developed by author for this material from Joint Publication 1–02: "Tactics: The employment and ordered arrangement of forces in relation to each other" and from the materials studied for employment of TD.

ensure their employed in this conflict from the depths to the front lines. They also guide how to achieve coordination, synchronization and prioritization, concentration and decentralization, division of sectors and airspace, tasks, rules of engagement, etc., without forgetting their protection from threats and techniques that the adversary uses against them. Tactics are integrated and synchronized across a wide range of tasks which we saw above such as conducting surveillance, intelligence gathering, early warning, and precision strike reconnaissance, EW, etc. This synchronization has great importance, for example, sync with EW units, which has tasks to counter adversary drone activity in one sector and if this task is executed without coordination with the drone units, there will be loss of friendly TDs from this attack. As an example of tactics, we will bring here the coordination of UAV units with those of EW during the Ukrainian offensive in the Kursk Region in the summer of 2024[68]. First, Ukrainian EW units with short-range jammers attacked Russian electromagnetic spectrum, bringing down UAVs though attacking drone control frequencies or repelling Russian reconnaissance drones in the area of operation. Meanwhile, Ukrainian drones were operating on frequencies that were not attacked or switched in the air in order to continue their mission. These EW attacks effectively blinded commanders to what was happening on battlefields and prevented them from reacting and attacking Ukrainian offensive and reconnaissance units with FPV drones and artillery, aviation. Also, this created shock and uncertainty while the Ukrainian ground force units advanced, crossed the front and attacked the Russian troops in the rear or flank.

Techniques are actions that are expected to be performed by the personnel and formations that have UAV in their structures. They are generally not specific instructions on how to perform certain missions, functions, or tasks[69]. They usually contain identified tasks that must be fulfilled after the order of the superior commands are released, but without specifying how they must be executed. The identified tasks should be detailed to allow for the use of UAVs more effectively, economy, and for coordination with parallel and superior structures, as well as subordinate ones. This process is helpful due to wide range of UAVs in Brigades (operational formations) and Battalions (tactical formations) for Ukraine and Divisions and Regiments for Russia. The techniques for employing TDs must be prepared on how the list of priorities/tasks will be completed from the drone unit, in accordance with goals of units they are as part of organically or attached to. And this thing in terms of importance and the role of unit, synchronization and cooperation with the artillery of superior units and those at the front. Also, part of techniques is the percentage/ amount of the TD which must be fixed to fulfill the main tasks, e.g. for attack, ISR

[68] D. Hambling, "Ukraine's Kursk Offensive Blitzed Russia with Electronic Warfare and Drones", Forbes, Gusht, 2024

[69] Paraphrase is developing by author from Joint Publication 1–02: "Techniques: Are non-prescriptive ways or methods used to perform missions, functions, or tasks" and from the materials studied for employment of TD

and in artillery support, relay etc. The sharing of tasks according to priorities and sectors by UAV units according to the typology they have and the role they will play. To make the techniques more perceptible, we will see one *case study* for prioritizing the employment of long-range Tactical Drone (e.g. RAM II), against Russian medium-range anti-aircraft systems such as SA-22 Pantsir and SA-11/17 Buk. These AD systems have an operational range of 30 km against air vehicles and they are sited in the strip of 20 km to 40km from the front line. Also, in this strip are placed large-caliber and reactive artillery, depots, barracks and command posts etc. which were moved away from the vicinity of the front line after they were become target to small-range tactical drone. The priority of the TD units equipped with RAM-II drones is the degradation of the AD systems, because, firstly, they prevent Ukrainian aircraft/helicopters from execution the tasks of close air support (CAS) for the units of ground forces, as well as to medium reconnaissance drones (TB- 2 Bayraktar, UJ-22) that execute ISR tasks in this area. Second, these AD systems also create a protective umbrella for Russian troops and Russian attack aircraft. These fighter-bombers are successfully releasing precision-guided bombs named FAB glide-bombs that weighs 250/ 500/ 1000 kg. These bombs are also called miracle weapons by many analysts because thanks to them the Russians are advancing to the front[70]. FAB bombs are fitted with guidance-and-glide kits, with inertial and satellite navigation systems, ailerons, and actuators at its aft end, which turn them into precision-guided bombs. They are released by Russian aircraft at a distance of 40-80 km and at an altitude of 4-8 km, within the umbrellas created by the air defense systems. So the priority to degrade Russian air defense systems station on above mention strip by these RAM-II drone would prevent the use of Russian aviation for launching these precision-guided bombs against the Ukrainian fortified lines, consequently stopping the progress of the Russian troops.

Procedures are specific detailed instructions and/or guidelines for operating TDs by crew/units. Procedures attempt to answer the question "how" the tasks assigned. They include all the steps necessary to execute the tasks that are assigned[71]. The priority for procedures is to provide complete detailed instructions so any task can be executing correctly by each units and operators/pilot by following them. Also, those likely give directions how to structure and to divide area of responsibility of unit into air sectors with clear boundaries for subordinate groups/team of that unit, as well as clear orders of which units they will support, attached or communicate with. Clearly defined are rules of communication in the chain of command, for calling in artillery and coordinating with infantry units on the ground, as well as the sharing tasks and priorities of the targets to be attacked. In order to make perceptible procedures used for TD on this conflict we will see below another two case of studies from Russian-Ukraine conflict:

[70] J. Hoehn, W. Courtney "How Ukraine Can Defeat Russian Glide Bombs", RAND, 28.06.2024

[71] Joint Publication 1–02, "Procedures are standard, detailed steps that prescribe how to perform specific tasks".

Ukraine tactical attack drone units will monitor the aerial view produced by ISR drones and upon noticing the approach of the enemy's convoy, attack groups will launch into the air a relatively high number of tactical UAVs for reconnaissance, relay and attack drone with commander order or with initiative of the operators. According to the procedures, operators will direct attack UAV/FPVs at the first vehicle of Russian convoy, aiming to hit optical periscope, communication gear, engine and tank track[72] to take out of combat. These actions would likely stop the column/attack group by becoming static and vulnerable to the FPV drones, anti-tank missiles, artillery, etc. (Pic. 7). Even in the case when blocked armored vehicles try to leave cleared track by anti-tank mines from the mine-clearing tank or by engineer etc., they would fall into the anti-tank mines again released by the Baba Yaga drones. After the column is blocked, UAV operators would continue to coordinate with the artillery for assessment of barrage and correction of it, as well as to re-attack with other One-way Drones and bomber UAVs. Next step would be to attack the crew that abandoned tanks or armored vehicles. Also, infantry units that were in support of them, which are hidden around the vehicles or in trenches etc. Meanwhile ground force commanders and UAV units in operation centers/ command posts would continue monitoring approach roads to the battlefield through long-range ISR in case reinforcements are approaching then they would give order to attack them without giving them a chance to join with stopped convoy.

The procedures for the *Russians* units before attacking the Ukrainian fortifications would be as follows: in order to find the weak points in one fortified sector they would use a group of 2-3 well-integrated UAVs[73] and well-defined tasks as follows: an Orlan-10 or Zala drone, would perform reconnaissance at an altitude of 1-1.5 km, keeping the target under continuous surveillance and transmit the live video to the command center of the ground unit that have been tasked to attack a sector and even to the drone unit that have same tasks. The second one would be an EW drone (Orlan-10 with payloads for EW) to attack electromagnetic spectrum of Ukraine units and the third relay drone, to allow the group of drones to stay better connected even while flying around ground clutter, in urban areas, and rising terrain. To damage fortifications, protective nets, camouflage or other defensive measures, tactical drone units will attack them with several OWA drones e.g. VT-40 FPV one by one and continuously will evaluate and correct the attacks. Meanwhile, in the direction of the Ukrainian fortified position, are approaching infantry attack group with at least 4 members in order to avoid drawing attention into that sector of the front and to minimize the loss if they fell prey to the artillery, as well as the Ukrainian FPVs. Units in the fortified positions could not react effectively as they would be under continuous drone attack.

---

[72] ISW, "Ukraine and the Problem of Restoring Maneuver in Contemporary War", USA, p, 35. "*Ukrainian tactical attack drones targeted the optics, communications gear, engines, and tracks of Russian tanks to cause mobility or utility kills that forced the Russians to abandon*"

[73] "Orlan 10 Unmanned Aerial Vehicle", Air Force Technology, 2021,

Conclusions and Suggestions

The use of UASs have had an indisputable impact on the battlefield in the Russian-Ukrainian conflict, and TDs also, have brought success to the Ukrainian Armed Forces (UAF) by achieving tactical victories on the front, hindering the advance of Russian troops. TDs have provided around 86% of all targets that the Ukrainians Armed Forces attacked and they are credited for destruction of around 2/3 of the Russian tanks (about 1550 pieces). Thanks to modern technology and the simplicity of production and low cost, as well as their great effectiveness, UAVs have become the main topics in the discourses of military analysts and researchers about how they should be integrated into their military structures. Currently, under the constant threat of the evolution of EW these UAVs are being developed in two directions: First, switching to semi-autonomous flight in the last 1-2 km and second to fully autonomous from take-off to attack. The first ones take-off and fly towards the target and during the course of flight they are controlled by the operator and then in the last 1 km they pass autonomously for searching, finding and attacking even when they are under the attack of EW to the target without the need for communication with the ground station. The second one, fully autonomous, can take-off and be directed to the area of operation to start seeking targets and attack them even when UAVs are under the attack of EW, without communication with the ground station. To achieve this, the country's authorities have created a special data base for system of opponent. Fully autonomous UAV can identify found targets as friend or foe based on this data. But the main challenge is not to attack friendly forces. Of the two above, semi-autonomous ones are being developed more as they offer greater security at the moment.

Each country has a unique approach to how TDs will be integrated into their Armed Forces. Mainly NATO countries and non-members in our Region (Balkan) have started to arrange contracts for purchasing them, such as Greece, which plans to buy the US Switchblade 300/600 "one-way attack" TD. Serbia[74] will produce about 5,000 pieces of "one-way attack" tactical drones "Mosquito" model, as well as ISR "Vrabac" model. In order to produce drones in their country, Bosnia is offering facilities and support to foreign companies. Meanwhile USA[75] through the 101st Airborne Division is experimenting with TDs based on the lessons learned from the war in Ukraine. Also, Albania will receive a "significant" number "one-way attack" TDs from Turkey. Below are some lessons learned from TD employment in above conflict:

• Ukraine through employing TDs in warfare have created *new operational space* (air littoral) and achieving localized and temporary air superiority at low altitude/air littoral *at a given time and place,* and through it they are executing tasks that in the traditional concept were mainly performed by aviation of whom has Air Superiority at the front.

[74] Defense Mirror.com, "Serbia to make 5000 "Mosquito" Kamikaze Drones", 11.03.2024

[75] S. Skove, "Drones could guide every bit of an Army division's firepower, 101st CO says", Defense One, USA, 2024

• The *new operational space (*air littoral) has emerged as a critical new subdomain of warfare in which potential cost savings and precision capabilities are offered and this space will continue to play an increasingly important role in modern warfare.

• Employment of TDs in large numbers and with low cost can increase the uncertainty of achieving objectives for the adversary.

• The use of TDs at the tactical and operational level has made the battlefield almost transparent, from depth to frontline trenches, enabling commanders to have a very good Situational Awareness.

• TDs are already multi-role, multi-use and quite efficient on the battlefield, due to the capacities and capabilities, and they can hit targets in motion, sheltered, in fortifications and at the weak points of the armor vehicle along with attack helicopters or drones in the air with extraordinary precision. Also, they can find, correct flight course and follow the target manually or autonomously with the help of computer programs and Artificial Intelligence.

• Long-range TDs can attack targets at a distance of up to 40-50 km from the front line. Targets at this distance are mostly beyond artillery range and usually they had been attacked by aviation.

• TDs are able to attack important targets (DT/TST-Dynamic Target/Time Sensitive Target) alone or in cooperation with artillery in three minutes (previously two-to-three hours were required), through the decentralization of decision-making in the hands of local commanders or drone operators.

• The purchase of TDs for the Armed Forces should be carried out in packages in order to allow the progress of the technology on them and to have possibility of updating, as well as the integration in military structures to be realized in stages. Initially some units to be equipped and later some other units as they can have opportunity to be equipped with the latest technology.

• Integration of TDs in the structure of the Albania Armed Forces requires: conceptual, doctrinal and structural changes, as well as preparation of TTPs. Also, we have to make integration and coordination of them with other systems e.g. artillery, armored vehicles, and aviation etc. in order to increase their effectiveness.

• The training of operators should be given special importance and include exercise in the simulator and in practice in at Tactical and JOINT levels with the support of computer programs and Artificial Intelligence.

• Creation of an industrial model of national production of TDs capable of responding to the latest demands and technologies without creating massive 'stockpiles' which will soon lose capabilities in war due to the rapid change of technology and EW against them.

Bibliography:

1. STANAG 4671.
2. Jack Detsch "Ukraine's Cheap Drones Are Decimating Russia's Tanks But experts say they're not a long-term solution to a lack of artillery rounds" Foreign Policy Magazine, 2024; https://foreignpolicy.com/2024/04/09/drones-russia-tanks-ukraine-war-fpv-artillery/.
3. Jez Parkinson "Force Protection Considerations" JAPCC, 2020; https://www.japcc.org/wp-content/uploads/A-Comprehensive-Approach-to-Countering-Unmanned-Aircraft-Systems.pdf
4. Washington Post "Azerbaijan's drones owned the battlefield in Nagorno-Karabkh" USA 2020; www.washingtonpost.com
5. Osman Aksu "Offensive Counter-Air Operations" JAPCC; https://www.japcc.org/wp-content/uploads/A-Comprehensive-Approach-to-Countering-Unmanned-Aircraft-Systems.pdf
6. J. Rogers "Future Threats: Military UAS, Terrorist Drones, and the Dangers of the Second Drone Age", 2021, JAPCC.
7. M. L Khan "The Crowdfunded Drone War in Ukraine" USA, Nacional Interest, 2022.
8. Ch. Mamo, "Revitalizing Ukraine's Defense Sector, and with It, Its Military" Emerging Europe, 2021, https://emerging- europe.com/;
9. NATO fixed-wing UAS Classification (AEP-4671).
10. Frederick W. Kagan, Kimberly Kagan "Ukraine and the Problem of Restoring Maneuver in Contemporary War" Institute for the Study of War, USA, 2024..
11. David Hambling "Ukraine's Mysterious New "Rocket Drone" Will Target Russian Air Force" Forbes, 2024.
12. UK Civil Aviation Authority "https://www.caa.co.uk/drones/rules-and-categories-of-drone-flying/first-person-view-flying/
13. J L Parker, 'Mission Requirements and Aircraft Sizing', in 'Special Course on Fundamentals of Fighter Aircraft Design', NATO Advisory Group for Aerospace Research and Development, Report No. 740, 1987.
14. First-person view (radio control) https://en.wikipedia.org/wiki/First-erson_view_(radio_control)
15. Саня Козацький "FPV drones: weapons that changed the modern war", Militarnyi, UKR, 2023 https://mil.in.ua/en/articles/fpv-drones-weapons-that-changed-the-modern-war/
16. Maximillian K. Bremer, Kelly A. Grieco, "Air denial: The dangerous illusion

of decisive air superiority,", Airpower after Ukraine, Atlantic Council, 2022; https://www.atlan-ticcouncil.org/content-series/airpower-af-ter-ukraine/air-denial-the-dangerous-illu-sion-of-decisive-air-superiority.

17. NATO, "NATO definition of Air Superiority" https://nso.nato.int/natoterm/Term.mvc/Display?termGroupId=14181.
18. David Axe "The Russians Sent a Platoon of Grenade-Hurling Robotic Mini-Tanks into Battle. The Ukrainians Blew Up the 'Bots in the Usual Way: With Drones. Manned or unmanned" Forbes, 2024.
19. David Hambling "Ukrolancet Drones Blitz Russian Air Defenses" Forbes, 2024;
20. Sakshi Tiwari "Ukraine Showcases Its Indigenously-Built RAM II Loitering Munition at IDEX 2023, Close to The Russian Stall", The Eurasian Times, 2023;
21. Jack Watling, Oleksandr V Danylyuk, Nick Reynolds "Preliminary Lessons from Ukraine's Offensive Operations, 2022–23 "RUSI, 2024.
22. Oleksandra Molloy, "How are Drones Changing Modern Warfare?" Australian Research Centre, 2024; https://researchcentre.army.gov.au/library/land-power-forum/how-are-drones-changing-modern-warfare
23. Air Force Tactics, Techniques, and Procedures (AFTTP) 3-2.3.
24. John Hoehn, William Courtney "How Ukraine Can Defeat Russian Glide Bombs" RAND, 28.06.2024.
25. "Orlan 10 Unmanned Aerial Vehicle," Air Force Technology, 2021, https://www.airforce- technology.com/
26. David Hambling "Steel Hornets: Inside Ukraine's Amazon For Drone Bombs" Forbes, 2024; https://www.forbes.com/sites/davidhambling/2024/04/02/steel-hornets-ukraines-amazon-for-drone-bombs/
27. Ukrainian Military Portal "FPV drones: weapons that changed the modern war" 2023; https://mil.in.ua/en/articles/fpv-drones-weapons-that-changed-the-modern-war/
28. D. Max Ferguson & Russell Lemler "Understanding the Counterdrone Fight: Insights from Combat in Iraq and Syria" Modern War Institute, West Pont USA, 2024.
29. David Hambling "New Software Makes Everyone an Ace FPV Pilot" Forbes, 2024.
30. Mykola Olshchuk "Air Power in the Russian-Ukrainian War: Myths and Lessons learned" JAPCC Ed 35, 2023.
31. Duncan McCroy "Electronic Warfare in Ukraine" JAPCC, Ed 36, 2023.
32. Michael Kofman, Rob Lee, and Dara Massicot, "Hold, Build, and Strike:

A Vision for Rebuilding Ukraine's Advantage in 2024" War on the Rocks, 2024, https://warontherocks.com/2024/01/hold-buildand-strike-a-vision-for-rebuilding-ukrainesadvantage-in-2024/.

33. Valerii Zaluzhnyi "Modern positional warfare and how to win in it", The Economist, 2023; https://infographics.economist.com/2023/
34. Jack Watling, Nick Reynolds, "Stormbreak: Fighting Through Russian Defences in Ukraine's 2023 Offensive," RUSI, UK, 2023, https://www.rusi.org/explore-our-research/publications/special-resources/stormbreak-fighting-through-russian-defences-ukraines-2023-offensive
35. BBC "How are kamikaze drones being used by Russia and Ukraine?" 29 December 2023.
36. Adam. Lowther, Mahbube. K. Siddiki, "Unmanned aircraft systems Combat Drones in Ukraine" Air Space Operations Review 3, USA, 2022.
37. AeroVironment Switchblade https://en.wikipedia.org/wiki/AeroVironment_Switchblade.
38. Samuel Bendett, "Where Are Russia's Drones?" Defense One, 2022, https://www.defenseone.com/;
39. Justin Bronk, Nick Reynolds, Dr. Jack Watling "The Russian Air War and Ukrainian Requirements for Air Defence" RUSI, UK, 2022.
40. Boyko Nikolov "Russia produces about 167 FPV drones per hour, says Moscow" Bulgarian Military. 2024.
41. ORYX Blog "Attack on Europe: Documenting Ukrainian Equipment Losses During The Russian Invasion Of Ukraine" https://www.oryxspioenkop.com/2022/02/attack-on-europe-documenting-ukrainian.html.
42. David Hambling "Ukraine's Kursk Offensive Blitzed Russia with Electronic Warfare and Drones" Forbes, 2024.
43. David. Hambling "Russian Volunteer Group Claims to Make 1,000 FPV Kamikaze Drones a Day" Forbes, 2023.
44. Prakash Nanda, "US Military Academy Releases New Report On Fighting Kamikaze Drones; Suggests 3 Ways To Counter UAVs", Eurasian times, 2024, https://www.eurasiantimes.com/us-military-academy-releases-new-report/amp/
45. Tim Mahon, "Serbia "receives Repellent C-UAS systems and other combat assets from Russia, despite international sanctions", Unmanned Airspace, UK, 2024 "https://www.unmannedairspace.info/counter-uas-systems-and-policies/serbia-receives-repellent-counter-uas-systems-and-other-combat-assets-from-russia-despite-international-sanctions/
46. Mykhaylo Zabrodskyi, Dr. Jack Watling, Oleksandr V. Danylyuk, Nick Reynolds

"Preliminary Lessons in Conventional Warfighting from Russia's Invasion of Ukraine: February–July 2022" ISW, UK, 2022;

47. Dominika Kunertova "Drones have boots: Learning from Russia's war in Ukraine", Contemporary Security Policy, Volume 44, 2023, Issue 4, p. 582 https://www.tandfonline.com/doi/full/10.1080/13523260.2023.2262792?scroll=top&needAccess=true#abstract
48. Joint Publication 3-09 "Joint Fire Support", 10 April 2019
49. Defense Mirror.com "Serbia to make 5000 "Mosquito" Kamikaze Drones, 11.03.2024 https://www.defensemirror.com/news/36306/Serbia_to_Make5000 Mosquito Kamikaze_Drones
50. Sam Skove "Drones could guide every bit of an Army division's firepower, 101st CO says" Defense One, USA, May, 2024
51. Simon Hilton, "How Drone Support is Improving Artillery Firepower The eyes in the sky are reinventing long range weaponry", Polymer Nano Centrum, 2023, "https://blog.polymernanocentrum.cz/how-drone-support-is-improving-artillery-firepower/
52. Tom Cooper, 'Kropyva: Ukrainian Artillery Application', *Medium*, 19 June 2022, at: https://medium.com/@x_TomCooper_x/kropyva-ukrainian-artillery-application-e5c6161b6c0a
53. S. Joshi, "The war in Ukraine shows how technology is changing the battlefield", The Economist, 2023 https://www.economist.com/special-report/2023/07/03/the-war-in-ukraine-shows-how-technology-is-changing-the-battlefield
54. Aleksandra Molloy "Drones in Modern Warfare Lessons Learnt from the War in Ukraine" Australian Army Research Centre, 2024 https://researchcentre.army.gov.au/library/occasional-papers/drones-modern-warfare
55. Hunder, Zafra, Rao and Kiyada, 'How drone combat in Ukraine is changing warfare'. Reuters, 2024 https://www.reuters.com/graphics/UKRAINE-CRISIS/DRONES/dwpkeyjwkpm/
56. Jaroslav Maxa, "Air War over Ukraine: Lessons for Taiwan", Security Outlines, 2023 https://www.securityoutlines.cz/air-war-over-ukraine-lessons-for-taiwan/
57. Maximilian K. Bremer, Kelly A. Grieco, "The Air Littoral: Another Look," Parameters 51, no. 4 (Winter 2021–22): 68, https://press.armywarcollege.edu/
58. Lt. Gen. David Barno, Nora Bensahel, "Drones, the Air Littoral, and the Looming Irrelevance of the U.S. Air Force" War on the Rocks, USA, March 7, 2024, "https://warontherocks.com/2024/03/drones-the-air-littoral-and-the-looming-irrelevance-of-the-u-s-air-force/
59. Christian Mamo, "Revitalizing Ukraine's Defense Sector, and with It, Its Military," Emerging Europe, 2021.

THIRD RUBRIC

EDUCATION AND TRAINING

Strength through knowledge: the key role of professional military education in National Security of Albania

Colonel (R) Dr. Çlirim TOCI
Leadership and Management Department,
The Baltic Countries College, 12 Riia St, 51010, Tartu, Estonia

Abstract

In a rapidly changing world where national security challenges develop every day, Albania, as a NATO member since 2009, is in a constant search to develop and perfect its military education. This system is not merely a platform to learn war techniques and strategies, but a foundation to build and shape future military leaders who will face the challenges of a national and international complicated and unstoppable environment. As our great Albanian renaissance symbol Naim Frashëri stated: 'and the light of knowledge will always lead us forward', and as such we also ask that the light of knowledge guide our soldiers towards a safer and more stable future.

Professional Military Education (PME) in Albania aims to prepare individuals capable of defending national sovereignty and integrity through a deep understanding of traditional and non-traditional threats. Military training is a complex mission that requires adaptation to a constantly changing strategic environment. General Omar N. Bradley has emphasized that "leadership is irreplaceable" and this is the essence of the PMU, to prepare skilled and capable leaders who are the heart of national defense.

This article will address the role of the PME as a pillar of national security by building a prepared and committed military force. It will analyze the role of education in facing today's and future challenges and a continuous improvement of PME developments, based on the experiences and best practices of NATO member countries and the Baltic countries.

Keywords: Professional Military Education (PME), NATO, strategic environment, military education system, leadership skills, national security, etc.

1. The importance of professional military education: indispensable and necessity for the future

Albania's national security is a broad concept that includes many different aspects of the country's defense and well-being. One of the key factors in strengthening this security is Professional Military Education, which is essential for preparing individuals for military roles and responsibilities. PME includes a wide range of training and development, aimed at preparing individuals not only with technical and tactical knowledge, but also with strategic skills, critical thinking and leadership skills.

What do we mean by PME?

In such conditions, the preparation of the military should take on a special importance. Learning and knowledge are two concepts, which impact not only the preparation of the military but also the improvement and development of the Armed Forces (AF). As the former president of the USA, J.F. Kennedy has stated, "Leadership and learning are inseparable." This principle is fundamental in understanding the importance of PMU in the preparation of military leaders and in the development of AF.

The document approved by NATO in 2011, 'Generic Officer: Professional Military Education - Reference Curriculum', emphasizes that 'the fundamental purpose of education is to instill the desire and ability to learn constantly. According to Eric Hoffer 'education is not only intended to produce prepared people, but also to form individuals who love learning and continue to learn independently[1]. This approach to PME emphasizes the importance of developing critical thinking and problem-solving skills, which are essential for military and civilian AF personnel.

The role of PME in National Security.

PME is of strategic importance and serves as a cornerstone in national security of Albania. This education equips military leaders with the qualities and skills necessary to face and control the security challenges of the 21st century. Through PME, creative thinking is developed and knowledge is expanded, which are important for adapting and changing the security environment[2].

What is the connection and interaction between the PME and national security? This is a very important question which, in the first place, requires us to understand the connection between these two concepts and their impact on personnel preparation. PME is essential for Albania's National Security, as it provides the theoretical basis and practical skills necessary for the effective implementation of national defense policies. PME curriculum is often aligned with key strategic documents, ensuring that

[1] NATO (2011) 'Generic Officer Professional Military Education: Reference Curriculum', p.4.

[2] Mie Augier and Wayne Hughes (2019) 'Innovative Thinking: The Role of Professional Military Education', https://cimsec.org/innovative-thinking-the-role-of-professional-military-education/, found June 05 2024.

military leaders are prepared to support and implement national strategy[3]. This connection ensures that PME graduates are skilled not only in the knowledge of defense strategies, but also in their contribution to the development of these strategies.

Preparing military leaders for the new security environment.

A developed PME system plays an important role in preserving national values and preparing the military to protect the country's interests[4]. Through PME, military personnel gain the skills to determine national priorities and interests and uphold national security principles. Continuous education and adaptation to new challenges help ensure a well-trained and educated military that is ready to cope with the tensions and conflicts that may arise in the region and beyond.

In addition, PME plays an important role in preserving and appreciating national values. This system instills in the military personnel a sense of duty and responsibility in the protection of national values and the development of the country, which is closely related to the quality of the educational level of our compatriots. Through PME, the military will be able to determine priorities and national interests and support the fundamental principles of the rule of law and the defense of national security.

PME system recommended by NATO.

In 2011, NATO presented a proposal on the development and functioning of PME, aiming at supporting NATO and partner countries in building a functional system for military and civilian training. In the NATO recommended system (see table no. 1)[5], three levels of PME are presented. This proposal does not introduce and does not recommend how the preparation of military and civilians will be done at the fourth (last PME) level.

PME system in Albania and the Baltic countries includes the preparation of the fourth level. The lack of this level may firstly create uncertainty in understanding and functioning of PME and secondly how valuable this system will be for NATO and partner countries.

The lack of coordination or involvement of the fourth level can present, for example, to the AF of RA, difficulties in applying the proposed formula. The absence of the fourth level can create problems in the equivalence of educational programs and students who come from other countries to study in PME system of the Republic of Albania. In the next chapter, the reader will have the opportunity to get and understand more about the levels of PME in the AF of RA.

---

[3] S. Huffington, A Oler, and D Tretler (2021) ed 'A National Security Strategy Primer … The Assumptions pivotal to the National Security Strategy', National Defence University Press, Washington, D.C. p. 7.

[4] S. I Radda (2014) 'The Role of Education in Promoting National Security', Sociologica Department, Bayero University, Kano, Nigeria.

[5] NATO, PfP Consortium and Canada., Generic Officer Professional Military Education: Reference Curriculum, NATO publication 2011, p. 5-6.

Levels of Education	Functions	Ranks
Basic Officer Training Course	Capable of commanding troops at platoon level	OF1/OF2 (2nd Lieutenant/ Lieutenant)
Junior Officers	Capable of commanding troops at OF3/Major Company level	OF3/Major (newly promoted)
Medium/High Level	Designed to serve general staffs commands for battalion, brigade	OF3/OF4 (Experienced Major)/Ltc/COL)

Table no. 1: PME system recommended by NATO

PME system in College of the Baltic States.

The College of the Baltic States was established in 1999, as an important element in the growth and improvement of the training of officers and civilians from establishing countries such as: Estonia, Latvia and Lithuania. The former president of Estonia Mr. Lennart Mery at the opening ceremony of the college would emphasize three main tasks to follow in the preparation of students:

1) Building a closer cooperation between the three Baltic countries in dealing with security challenges.

2) Strengthening and better preparation of the structures of the armed forces.

3) Engagement with neighbors in creating peace in the region[6].

Since that time the College has a very important mission in preparing future leaders with the necessary qualities and creative skills with the best possible understanding of security challenges. The curriculum is designed to meet the complex challenges in the Baltic Sea region with a special focus on the Russian Federation, the role and interests of NATO and the EU[7].

PME in the Baltic countries includes a number of courses and programs of training and education for junior officers and senior officers. In PME system, there are four levels of preparation and development. The first and second levels provide the basic training and education of new officers. These levels of preparation are the responsibility of the Baltic countries. While the college is responsible for the third level (Commands and Joint Staffs course) and the fourth level senior course (command studies). This approach regarding the preparation and development of officers is presented in table no. 2[8].

[6] Corum J., Johanson A., (Quoted here) 20th Years of the Baltic Defence College: Professional Military Education in the Baltic States, Valipress OU Estonia, 2019, pp. 5.

[7] BALTDEFCOL, HCSC 2024 Course Plan (course plan), Tartu, Estonia, p. 5-6 & 20

[8] HCSC (Higher Command Studies curriculum development, (2024), Tartu, Estonia, p. 6.

Level 1	Level 2	Level 3	Level 4
Basic Level	Junior Officer	Advanced	Senior Level
Tactical Level	Tactical Level	Operational Level	Strategic Level
Basic Level and Specialty Courses	Captain's Course and Intermediate Course	Joint Command and Staff Course	Advanced Command Studies Course
National or international academy	National or international academy	Colleges Baltic States College or International or War Colleges	Colleges Baltic States College or International or War Colleges
OF 1 (2nd Lieutenant)	OF 1 – OF – 2 (2nd Lieutenant – Lieutenant)	OF 3 – OF 4 (Major – Ltc Colonel) and civilian	OF 4 – OF 5 (Lieutenant Colonel - Colonel) and civilian

Table no. 2 Baltic States PME system

2. Historical overview and vision of PME in AF

PME in Albania has a long and complex history, playing an essential role in preparing military troops for security challenges. The history begins from the period of the state of Arber, where noble families such as Ballshaj, Muzakaj, Dukagjini and Kastrioti maintained individually trained and paid armed forces to cope with war situations. In special cases, these families contributed to the army of the country of Arber. More specifically, the origin of the development of military education begins in the years 1797-1822, where the Paschal of Ioannina, led by Ali Pasha Tepelena, in Bonilë, established the first school of artillery, engineering and cavalry, with the participation of French, Italian and Albanians.

By the end of the 19th century, Albania faced great challenges from the Ottoman Empire and the ambitions of the Russian Empire. During this period, the League of Prizren (1878) was created, which aimed to protect the Albanian territories and create an independent state. The League organized and mobilized military forces, although it faced great difficulties. After the declaration of independence in 1912, Albanian soldiers were mainly trained in Ottoman schools. During the First World War (1913-1919), countries such as Austria-Hungary, Italy and France contributed to the training of Albanian military. In 1919, the provisional government opened a school for the training of officers and gendarmes. Institutionally, the first military school was established on October 26, 1926.

From 1920 to 1939, there were schools operating in Albania that offered six-month courses for the preparation of officers. The Albanian Kingdom of that time established the school for the training of military in 1928. Whereas, during the Second World War, the National Liberation Army (NLA) prepared its cadres in difficult conditions,

according to combat needs. After the liberation of Albania on November 29, 1944, the local authorities of that time decided to create the bases of military education, establishing on November 8, 1944 the (Shkollën e Bashkuar të Oficerëve) United Officers' School, which later received the name "Enver Hoxha". This school trained officers for infantry, artillery, and logistic. Also, in Vlora, schools were opened for the preparation of naval and aviation officers. While Skënderbej Military High School was established on March 28, 1945, for the preparation of young partisans.

The final decision was made on May 10, 1958, creating the legal basis for the establishment of the Military High School. Later on September 15, 1961, by government decision, it was named the Military Academy. The Military or Defense Academy has provided advanced and strategic qualifications for officers from 1958 to the present day. But what was actually the PME system before the 90s, in Albania. Below you will be able to see picture no. 1.

Picture no. 1: Structure of PME (1944-1992)

3. Professional Military Education in the Republic of Albania after 1992

Let's start with the question: What is the mission of Professional Education in Albania?

PME in Albania aims to form a corps of capable leaders, officers and non-commissioned officers, prepared to successfully carry out the assigned tasks and serve the nation. These leaders must be equipped with the skills to think and analyze critically and creatively about leading AF, interacting with NATO allies, and dealing with the risks posed by potential adversaries. The personnel military training and devotion to the homeland and the nation are the main objectives of the PME's mission and goals in the Republic of Albania. Professional military education in Albania is an integral part of the national education system. The main institutions that deal with the education of military (officers and non-commissioned officers) and civilians are the Armed Forces Academy (AFA) and the Defense and Security College (DSC). These institutions aim to educate and train military and civilians at all levels of management of the AF and other local institutions dealing with security and defense issues. The mission of military education is essential to understanding the nature and preparatory capabilities of these institutions[9].

[9] AFA Status, 2017.

Preparation objectives.

According to the status of the Armed Forces Academy approved in 2017, the objectives and tasks for the development and progress of military education in the Republic of Albania have been determined. Academies are tasked with preparing and educating military and civilian personnel at all levels of the AF. This includes military education at the first, second, third and fourth levels. AFA offers Bachelor's, Master's (in Arts or Sciences) and doctoral studies. The Defense and Security College prepares officers from the rank of Captain to the rank of Colonel, passing from the second to the fourth level of the PME.

Importance of Curriculum in Military Education.

Curriculum compilation plays an essential role in the smooth running of the learning process and in achieving the educational objectives of the military student troops. Curriculum significantly influences various aspects of philosophy, psychology and sociology, being an essential, complex and important element for pedagogy. The main purpose of the curriculum is to develop the learning process and prepare military students to meet their learning objectives.

AFA and DSC (KMS) should focus on improving and updating the curriculum, with the aim of adapting to contemporary risks and understanding the security environment, which is becoming more and more unpredictable. To achieve this, the curriculum must be reviewed annually and changed according to a percentage determined by law or internal regulations (SOP)[10] of military educational institutions. This requires strong support from superior institutions, such as the Ministry of Defense (MoD) and the General Staff of the Armed Forces (SHPFA), morally, financially and materially, to ensure a healthy and sustainable education system.

The initiative of the Government of Albania for the improvement of PME.

In 2021, the Government of Albania and the Ministry of Defense declared that they will pay more attention to training and education in the field of defense. This initiative aims to utilize two main sources: (1) the experience within the Armed Forces and (2) the experience of the most developed NATO member countries. Albania has sent and trained a large number of military personnel to the most famous military academies of the USA, the United Kingdom, Germany, Italy, Turkey, Greece and other countries, benefiting from the experience and relations established with similar institutions. These experiences and relationships will contribute to the reformation and improvement of the military education system in Albania.

Overview of Professional Military Education.

Professional Military Education prepares officers in four main levels or areas:

First level - Focuses on the preparation of new officers, the responsibility of the

[10] SOP – Standard Operating Procedure

Armed Forces Academy. In the past, this level was associated with the "Skënderbej" Military Academy.

Second, third and fourth levels - All other levels should be the responsibility of the Defense and Security College. These levels include tactical, operational and strategic training of officers (See table no. 3).

Professional Military Education in the Armed Forces of the Republic of Albania.

Level 1	**Level 2**	**Level 3**	**Level 4**
Basic Level (*Bachelor Program - 3 years*) cadet / student	Junior Officer	Advanced	Senior Level
Tactical Level	Tactical Level	Operational Level	Strategic Level
Other new officer preparation courses (*contingent from UT – 9 months course*)	Basic Staff Officer Course **(KTHOSH)**	- Command and General Staff Course **(KKSHP).** - Senior Officer course **(KLO)**	Senior Security and Defense Course **(KLSM)**
Responsible institution: Armed Forces Academy	**Responsible institution:** Defense and Security College	**Responsible institution:** Defense and Security College	**Responsible institution:** Defense and Security College
OF 1 (2nd Lieutenant, Lieutenant)	OF – 2 (Captain)	OF 3 – OF 4 (Major – Ltc Colonel) and civilian	OF 4 – OF 5 (Lieutenant Colonel – Colonel) and civilian
(Master *Programs Masters (MA & MSc) & doctorates (PhD)*) **Responsible institution** : Armed Forces Academy			

Table no. 3. Armed Forces Academy/ Defense and Security College

4. Challenges and expectations for the future

AFA deals with the education of military students/cadets, while Defense and Security College conducts several courses, such as the Basic Staff Officer Course (KTHOSH), the Command and General Staff Course (KKSHP), the Senior Officer Course (KLO) and the Senior Security and Defense Course (KLSM). These courses are designed to prepare military personnel with ranks OF2/OF3/OF4 and OF5. As

the security environment and military art change, the curriculum must adapt to the changes. In this context, several key questions arise that require answers:

• What needs to be improved in AFA and DSC?

• How should the education system be built?

• What will be the financial and human resources?

To improve AFA and DSC, some measures are necessary:

- **Development of the structure**: The current structure must continue to develop, not change (evolution not revolution). It is necessary for the academic staff to be evaluated and refreshed.

- Curriculum and literature enrichment: Literature (both in print and online) should be enriched to reflect the latest developments in the military and security fields.

- Review of the third level of military education: The third level of education should be reviewed in accordance with the NATO member countries practices. The law governing the defense education system may need to be amended to reflect these developments and technological advances.

Necessary changes in DSC courses.

The Command and General Staff Course (KKSHP) and the Senior Officer Course (KLO) constitute the third level of education in the field of defense. There is a need for change and improvement here. The best experiences of Western countries and the Baltic College offer models that can be adapted to the Albanian environment. For example, DSC could integrate the KKSHP and the KLO into a joint course called the Joint Command and General Staff Course (JCHC).

This integrated course will save time and financial resources and adapt the curriculum to reflect changes in the nature of warfare and the security environment. The new course will last no more than 10-11 months. Whereas some parts of the KKSHP program can be transferred to the Basic Staff Officer Course (KTHOSH) extending this course from 4 to 5-6 months, in accordance with the standards of the Baltic countries. Whereas, the Senior Security and Defense Course (KLSM) should last around 5 months or 23 weeks, covering a wide range of topics in the field of security and defense, such as international security environment, NATO/Russia, defense policy, defense planning/planning (strategic) and management, risk prevention, etc. This will involve more actors from inside and outside the country.

Academic Staff and Research Work in AFA and DSC.

AFA and DSC must have an academic cadre prepared with the best standards at home and abroad. Knowledge of English language is essential to absorb the necessary information and knowledge. The institution should be considered as the backbone of AF. Without it, there is no sustainable development and national security.

In order to raise the quality of education, it is essential to improve the evaluation of academic staff. Those serving in AFA and DSC must be among the best and have an edge over others in the system. Without a quality academic cadre, there are no trained military. Nelson Mandela says: *Education is the most powerful weapon with which you can change the world.* The inner world of AF and its members. *The aim of professional military education,* as Louis Simpson says, *should not be just to prepare men for war, but for a longer term.*

AFA and DSC should have an internal communication system (intranet/computer network) to facilitate communication with academic staff and students. For example, the Baltic College uses ILIAS (software) for internal communication. Likewise, the official website of AFA and DSC should be self-managed and provide the necessary information for the public and the academic community.

Military education institutions should be a model not only in the field of education, but also of the values it carries. Today, we need military with knowledge not only in the field of defense and security, but also in politics or in the field of economy. To illustrate, I want to cite a quote from Colonel Lincoln in a letter to his former trainer at West Point: *'I am beginning to think that we need a model of the staff officer who has three heads—one for politics, one for economics and one for military affairs.'*[11]

Conclusions

Building and improving performance in academic institutions in the field of defense requires will, support and transparency. Military academies are responsible for preparing military personnel with the necessary knowledge and skills at all levels of the PME. Implementation of educational policies and academic curriculum requires two main things: adequate infrastructure and educated academic staff. Achieving these objectives requires investment and attention to personnel *(invest in people)*. Military academies must prepare creative minds that will lead combat units and formations according to NATO standards.

The PME must compile and enable updated curriculum, according to the requirements and standards dictated by technological developments and security environment. The revised and improved curriculum should create an attractive and quality academic environment for the acquisition of knowledge and new combat methods and coping with risks. In an increasingly unpredictable security environment, military academies are places where the risks and challenges of the 21st century can be internalized and debated. Cyber warfare and disinformation are dominating the security environment and national security, and we must be prepared for these challenges. This is achieved through standardized institutions and trained teaching staff.

[11] Fred Kaplan (2014) '*The Insurgents: David Petraeus and the Plot to Change the American Way of War*', Simon & Schuster Paperbacks, New York, pp.6.

Educated military and critical thinking will make it easier to understand the security environment and deal with risks. PME will always be influenced by new challenges and opportunities. We need to understand what we want to learn at the Academy, who should come to AFA and DSC and who should prepare them? The reformation objective should be the improvement of academic environment and the changes should be effective and necessary. While we may change or restructure military education institutions, the preparation of the academic cadre remains essential. Without a trained teaching staff, any effort is destined to fail. Educators and instructors are the *"Achilles' heel"* in the reformation and progress of military education institutions.

This article does not claim to provide answers or solutions for the best model or system of preparation in the field of PME in the Armed Forces of the Republic of Albania. Academic staff, curriculum designers, and military education experts can provide more accurate answers. We must all agree that military academies and colleges must take their rightful place. AFA and DSC will be the cornerstone in shaping and preparing the military with the necessary knowledge and skills to protect the country and face risks. We must build systems that will stand the test of time.

References

1. Mie Augier and Wayne Hughes (2019) *Innovative Thinking: The Role of Professional Military Education*, https://cimsec.org/innovative-thinking-the-role-of-professional-military-education/, June 05, 2024.
2. S. Huffington, A Oler, and D Tretler ed. *A National Security Strategy Primer … The Assumptions pivotal to the National Security Strategy*, National Defence University Press, Washington, D.C. (2021).
3. S. I Radda, *The Role of Education in Promoting National Security*, Sociologica Department, Bayero University, Kano, Nigeria, (2014).
4. NATO, PfP Consortium and Canada., Generic Officer Professional Military Education: Reference Curriculum, NATO publication 2011, p. 5-6.
5. Corum J., Johanson A., *20th Years of the Baltic Defence College: Professional Military Education in the Baltic States*, Valipress OU Estonia, 2019, pp. 5.
6. HCSC (Higher Command Studies Course), curriculum development, (2024), Tartu, Estoni, pp. 6.
7. Sabri Godo, *Ali Pasha*, Tirana, 1989, pp. 111, 142-146.
8. Fred Kaplan '*The Insurgents: David Petraeus and the Plot to Change the American Way of War*', Simon & Schuster Paperbacks, New York, (2014).
9. Rupert Smith '*The Utility of Force: The Art of War in the Modern World*', Penguin, London, (2009).

Building Public Relations Online by President of Ukraine Volodymyr Zelenskyy[1]

Msc. Edlira PRENDI
Faculty of Defense and Security, AAF

Abstract

The war in Ukraine has captured the attention of international public opinion. Since February 24, 2022, Ukraine has consistently dominated headlines around the world. This is due not only to the media's commitment to reporting on the situation, but also to Ukrainian President Volodymyr Zelenskyy's decision to communicate directly and immediately with the public through all available communication channels.

Public relations have taken on an international dimension, and world leaders are placing special importance on global public communication. Military communications are more prominent than ever on the international stage, since the Cold War. It is important to understand how Public Relations have evolved in the international arena: in what form they are conducted, who they are addressed to, why they target foreign audiences, and why public opinion is crucial in times of war.

This study aims to present the results of research on the public communication of the President of Ukraine, who is currently the most prominent figure in international public discourse. Also it was made possible through qualitative research and analysis of findings, combined with quantitative research, as detailed monitoring and analysis were conducted across all communication channels of President Zelenskyy and the institution of the Presidency.

This study highlights the fact that the development of technology and social media plays an essential role in building a successful international image.

Keywords: international public communication, public relations, V. Zelenskyy, soft power, digital media diplomacy.

[1] Case study of international image building and public relations in wartime.

Introduction

This study aims to present the results of research on the public communication of the President of Ukraine, Volodymyr Zelenskyy, who is currently the most prominent man in international public discourse. Zelenskyy has become a unifying figure not only for the people of Ukraine, who are facing the invader, but also for the majority of international public opinion. He is viewed as the person who symbolizes the global struggle between democracy and totalitarian regimes.

Since February 24, 2022, Ukraine has dominated international media headlines. This is due to the media's commitment to reporting on the situation in Ukraine, as well as President Volodymyr Zelenskyy's decision to communicate directly and immediately with the public through all available communication channels.

For the first time, a leader - specifically the President of Ukraine - is attempting to build direct communication with citizens from different countries by speaking in their respective languages. In English, Zelenskyy addresses the elite and journalists, but he makes a point of speaking to everyone in their own languages as well.[2]

From the very first days of the war, he has launched an intensive and well-organized strategic communications campaign aimed at all audiences, including the Russian people, to secure support for Ukraine and condemn Russia for its attack. Only 38 hours after the attack he chose to respond with a direct and frontal communication strategy.[3] He did this specifically to send the clear message that Ukraine would fight and not surrender in the face of Russia's military offensive. This was an important message not only for the people of Ukraine, but also for Russia, which had expected Zelenskyy to flee the capital, and for the Western world, whose experts had predicted that Ukraine would capitulate within hours.[4]

Equally important was another piece of news that quickly spread around the world, reinforcing the message that Ukraine would fight. Through these messages, Zelenskyy became the most emblematic figure of the war taking place in this part of Europe. The war in Ukraine changed the agenda of other governments and multinational organizations, both in the fields of security and defense and in the area of human rights.

By physically staying in Ukraine, Volodymyr Zelenskyy launched the most powerful offensive ever undertaken by a leader to communicate with the entire world. He used technology to participate at all international meetings, to deliver speeches in numerous parliaments and dominate social media platforms. It must be acknowledged that technology and its use have taken on a new dimension during the course of the war in Ukraine.

[2] Refer to the videos on the YouTube channel.

[3] Zelenskyy addressed the nation and the world with a video speech from Kyiv in the courtyard of a government building and assured the people that the government had not capitulated.

[4] Interview with the ambassador of Ukraine in Tirana.

President Zelenskyy used every available means of communication to tell the world what was happening in his country. Dressed in military uniform, with a tired face and sleepless, unshaven, he used non-verbal communication to capture attention, especially on social media platforms.

Study Purpose

The purpose of this study is to understand how public communication is changing due to social media. Today, public relations are increasingly developing online, surpassing traditional communication formats as secondary. This study helps us understand how technology has transformed public relations during times of major international crises, such as the war in Ukraine.

Nearly 30 years ago, traditional media were the primary sources reporting on wars and developments on the ground. Public communication did not have the same scope or significance at that time. Public relations now rely heavily on media and technology to be effective, and both of these elements have changed drastically. They have become faster, more pervasive and easier to access. Public relations have also taken on an international dimension, with leaders placing increasing importance on foreign public communication. It is crucial to understand how these changes have reshaped public relations in the international arena. In what forms is public communication conducted now? Who is the target audience? Why are foreign audiences the focus? And why is public opinion especially important during times of war?

Military communications have returned to public discourse[5] and are more prominent than ever on the international stage, especially since the Cold War and, more specifically, the Kosovo War. However, military communications in Albania remain understudied. Since 2008, when Albania became a member of NATO, the world's largest political-military alliance, there has been a noticeable increase in attention to civil-military cooperation during peacetime.

Such studies are important to conduct in our country as well. Despite its geographical distance, Albania is a NATO member and is directly affected by every crisis. Unlike leaders of other Balkan countries, such as Serbia, Bosnia and Herzegovina, Albanian leaders reacted swiftly by imposing sanctions on Russia. The paper helps practitioners of public relations and media to understand that military communication is crucial to grasp and comprehend properly, especially in regions like the Balkans where conflicts have not yet been fully resolved. In times of war, shaping the country's international image becomes vital for its future.

The study analyzes how the President of Ukraine built online public relations, the strategies and tactics used in communication and the role technology played in their interaction.

[5] The author of this study during the years 2013-2017 was engaged in the Ministry of Defense of Republic of Albania, in the position of Communication Advisor. This was one of the motivations to undertake this study.

Theoretical basis

In the context of this paper, both foreign and Albanian authors have been referenced. This study draws on their qualitative perspectives, with a particular focus on the works of the Catalan scholar Manuel Castells, especially his book "*The Power of Communication*".

Joseph Nye's concept of *Soft Power*, although rooted in international relations, finds a relevant application in Ukraine.

Albanian academic Artan Fuga is included in this study to explain propaganda as one of the challenges Ukraine is likely to face.

The scholar Alban Tartari contributed to the development of communication campaigns, while scholar Hasan Saliu focused on the concepts and practices of Public Diplomacy.

Methodology

The methodology used in this study is qualitative research, complemented by the analysis of the findings. There is also an overlap with quantitative research, as detailed monitoring and analysis were conducted across all communication channels of President Zelenskyy and his institution.

Since the study focuses on President Zelenskyy's online communication, detailed monitoring of the official website of the Presidency of Ukraine was conducted over a 10-month period (February-December 2022). This monitoring focused on meetings, as well as bilateral and multilateral visits held in Kyiv, Ukraine, during this time. The agendas of speeches delivered by President Zelenskyy in various parliaments around the world, as well as his interviews with international media were also monitored.

In the framework of this study, the social networks *Facebook* and *Instagram* were monitored over the same time periods throughout 2022. A comparison between the two was made, and the trends in interactivity on each platform during the monitoring periods were highlighted. Two *YouTube* accounts were monitored: one corresponding to the office of the President of Ukraine and another created by the President's team.

This study includes six interviews with experts in the field. Among them are international communication experts, former foreign ministers, journalists who have reported from the front lines of the war, and representatives of the diplomatic corps in Kyiv and Tirana. The interviews were designed to provide both professional and personal perspectives on the subject of this study, drawing on the participants' experience and expertise.

Research questions and hypotheses

To better understand how the President of Ukraine, Volodymyr Zelenskyy, communicates with the governments of other countries around the world and with international institutions, as well as to explore his strategy and tactics in international

public communication, research questions and preliminary hypotheses have been formulated, presented in the sections of the paper.

Public Relations in wartime

Ukrainian President Volodymyr Zelenskyy uses every available communication channel to convey political and military messages. He has developed an intensive communication strategy targeting:

the international community, the people and the military of Ukraine, the people and government of Russia. To ensure the message effectively reaches its intended audience and achieves the desired impact, Zelenskyy employs every available form and channel of communication.

Face-to-face meetings are crucial in public relations. Meetings of this nature have always been important,[6]as they convey key verbal messages but more importantly, they communicate through non-verbal language.

A person's ability to convey messages through non-verbal behaviors and to interpret messages communicated non-verbally is also influenced by their profession and the level of their professional skills.

"Politicians and diplomats frequently leverage the advantages of non-verbal communication to express unofficial political orientations, particularly to convey messages with multiple meanings—ambiguous statements about policies that are expected to become clearer over time."[7]

The scholar Manuel Castells also spoke about the importance of non-verbal language, noting that "most communication is built around metaphors because this is the way to enter the brain, activating the appropriate brain networks that will be stimulated in the communication process."[8]

The President of Ukraine has masterfully used technology to communicate virtually with citizens around the world and leaders of many countries, delivering speeches in national parliaments. More than to parliamentarians, Zelenskyy's most important messages are addressed to the people of those countries.

Empathy and emotion are very important elements in public relations, and Zelenskyy has sought to evoke these feelings through his speeches. During his speeches in national parliaments, he has often drawn parallels between the history of his country and the country he is addressing.

---

[6] It is enough to recall the novel of the writer Ismail Kadare "Dimri i Vetmise se Madhe", (Winter of the Great Loliness), which talks about the meeting of E. Hoxha with Nikita Khrushchev. The movie "Balle per Balle " (Face to Face) also refers to the novel in question.

[7] *Zyhdi* Dervishi*, Lente të ndërveprimit simbolik:analizë sociologjike e rolit të simboleve kulturore, të komunikimit joverbal.* Tirana: Ermal. 2016, page 134.

[8] Manual Castells, Communication Power. New York: Oxford University Press, 2009, page 143.

Public relations need to be as truthful and reliable as possible in order to achieve the desired impact. In this regard, the First Lady, Olena Zelenska, has also played an important role. Her involvement and intentions help the message resonate more deeply with public opinion. Women tend to stay away from war, but when it happens, they convey it more as mothers, sisters and wives.

Diplomatic Communication

The President of Ukraine has used every diplomatic tool and every communication channel available to convey his message to the international audience. In this regard, he has maximized the use of technology to serve his communicative agenda. He has organized his diplomatic agenda in order to reach even the most indifferent audience.

Zelenskyy's axis of diplomatic communication operates in three specific directions:

- Diplomatic visits to Kyiv by various leaders. During 2022, Kyiv hosted 59 official visits.
- Discussions in the parliaments of different countries. President Zelenskyy virtually addressed 31 parliaments around the world during 2022, without moving a single day from Ukraine.
- Presence at events of international organizations, security forums, academic environments, music and cinematography festivals around the world. Each of these platforms has provided Zelenskyy with the opportunity to target specific audiences with relevant messages.

Online communication

Volodymyr Zelenskyy entered politics from the world of entertainment, and as such, he is undoubtedly an extraordinary communicator, whose skills have been honed over decades in the entertainment industry. The President of Ukraine has built an entire communication infrastructure with the world, which he has perfected during the war.

Zelenskyy skillfully leverages the advantages he creates:

The online world, as he communicates with the parliaments of different countries, international organizations, the academic community, the business world, and more.

Social networks, through which he engages with specific audiences.

Video distribution platforms are used to deliver his message in the language of the target audience.

Volodymyr Zelenskyy focuses his communication primarily on daily reports about the war, telephone or virtual communications with international counterparts, field visits to military troops in Kyiv as well as outside the city, staff meetings, and more.

In Zelenskyy's communications there is no information regarding the human losses Ukraine is suffering. "The only thing they have done is maintaining the morale of Ukraine by providing detailed information every day. There is given

detailed information about Russia's losses, even their total number. Meanwhile, no information is given about the losses of the Ukrainian Army," - reports journalist Kasapi based on his more than two-week stay in Ukraine.

Scholar Alban Tartari notes, "Based on the audience being addressed, the message is also constructed. The golden rule of public relations is that the message should be crafted in such a way that it is understood the first time by the target audience."[9] Zelenskyy is the best example of how he strategically constructs his message depending on the audience he is addressing. In his communication on social networks, Zelenskyy also takes into account the number of followers, preferences, age and tailors the message based on these specifications.

The two authors of the book "The Zelenskyy Effect", Olga Onuch, Professor of Politics at the University of Manchester, and Henry E. Hale, Professor of Political Science and International Relations at George Washington University, study Zelenskyy's communication skills and their impact during the war. The scholars argue that his speeches are designed to be easily understood by ordinary Ukrainians, and delivering them through short videos on social media makes them even more effective.

Communication through videos by President Zelenskyy is a form that meets the demands imposed by social networks. In the book The Hype Machine, Sinan Aral[10] states that "online social networks, instant messaging, collective knowledge production, and newsgathering technologies have fundamentally changed the way information is produced, distributed, consumed, used, and evaluated."

For the scholar of public relations, Alban Tartari, "what has changed are the media and technology - two tools through which public relations is applied and which enable the distribution of messages, content, and meanings in this field. In addition, those who consume the messages have changed: the public, who now face, receive, and process more information than previous generations, often much more than their grandparents."[11]

When it comes to attracting international attention, Volodymyr Zelenskyy leaves nothing to chance. The President communicates at least three times a day, and there have been days when up to 19 posts[12] were made on his Instagram account. It is worth noting that Zelenskyy is especially active on *Instagram*, with an average of 8 to 10 posts per day during the monitored period.

Content of Messages:

The President of Ukraine has based his public communication around five key topics, which have had a significant impact on public opinion.

---

[9] Alban Tartari, *Marredheniet me Publikun*, Tirana: LUIS PRINT, 2021, page 179.

[10] Sinan Aral, *The Hype Machine.* New York: Penguin Random House LLC., 2020, page 17

[11] Alban Tartari, *Marredheniet me Publikun***,** Tirana: LUIS PRINT, 2021, page 39.

[12] Instagram posts of President Volodymyr Zelenskyy on February 3, 2022.

First, Zelenskyy always addresses all citizens of Ukraine, referring to them as the citizens of a Great Nation. Second, he frequently makes statements emphasizing the unity of Ukraine. Criticism of the Elite: He consistently criticizes the political and economic elite for failing to do enough. Ukrainian Values: Zelenskyy often highlights Ukrainian values, which he defines as European, democratic, civic, liberal, and inclusive. He contrasts these with the value systems of the Kremlin and the oligarchs. National Responsibility: He consistently links personal responsibility to national duty.”[13] The selection of messages conveyed to the audience becomes particularly important when you want to direct their attention toward a specific interest or objective for which the communication is intended. The concept of “framing” stands out, which, according to Castells, refers to an action carried out through processes that unfold in the media. “Framing,” as the action chosen by the sender of the message, is sometimes random and sometimes intuitive, but it establishes a direct connection between the message, the receiver (the brain), and the subsequent action.”[14]

In his book “A Message from Ukraine,”[15] Volodymyr Zelenskyy summarizes some of his most important speeches from the years 2019-2022. The book is divided into four chapters: the first discusses the values that Ukraine represents; the second focuses on speeches about the war; the third addresses the demands of Ukraine, serving as its voice; and the final chapter is dedicated to the nation of Ukraine.

On March 8, 2022, Volodymyr Zelenskyy delivered a video speech to the UK Parliament. This marked the moment when Zelenskyy opened another front in the war with Russia - the war of communication. In the six months that followed, Zelenskyy would give hundreds of speeches around the world. Across every communication platform, he emphasized the need for the world to provide military support to Ukraine and impose sanctions on Russia, in support of “the values of democracy and freedom.”[16]

The Albanian Consul in Ukraine, Shakhin Omarov, believes that ‘the essence of communication lies not in the channels or technical devices themselves, but in the content and the manner of communication: he speaks on his own behalf, using simple language to convey essential matters, and remains closely connected to the people.”[17]

The scholar Artan Fuga in his work *“Mediamorphosis and Metacommunication,”*[18] refers to the 19th-century Italian philosopher who, observing the country and the

[13] Olga Onuch & Henry E. Hale, *The Zelensky Effect*, United Kingdom: Hurst&Company, London, 2022, page. 247-248.

[14] ManualCastells, *Communication Power*, Oxford: Oxford University Press Inc., 2009, page 158.

[15] Volodymyr Zelensky, *A message from Ukraine,* London: Hutchinson Heinemann, Penguin Random House UK, 2022.

[16] Ibid, page 63.

[17] Refer to the interview with the Albanian Consul in Ukraine.

[18] Artan Fuga, Mediamorfoze and Metakomunikim, Tirana: PAPIRUS, 2017, page 405

Italians as fragmented and lacking the sense of collective identity, argued that a war was necessary to unite them psychologically as a nation. "It doesn't matter if we win this war. It is even better if we lose it, because with the feeling of being humiliated by foreigners, with the sense of shared shame, we will strengthen our bonds and feel part of a common nation".

Equipped with a sense of the strength of a united nation, as early as April 2022 and beyond, the President of Ukraine made a significant shift in public communication, particularly in the messages he conveyed to political leaders, especially Russia. As a result, Zelenskyy's rhetoric evolved, transitioning from a call for peace to a demand for victory. Zelenskyy's communication is also regarded as a compelling form by former Foreign Minister Ditmir Bushati, who discusses the interplay of two elements - "resistance and victimization" - which convey a message of global solidarity. Bushati believes that "Zelenskyy's primary objective has not been to frame the war as one merely for the protection of Ukraine from Russian aggression, but rather as a defense of the values and principles upon which a united Europe is built"[19]

"The narrative that Ukraine is protecting Europe is a powerful one, especially in countries like neighboring Poland, which feels the real threat of war. In this regard, it is sufficient to mention the increased frequency of visits and communications between the Ukrainian and Polish governments during the war," says Adam Richardt, editor-in-chief of New Eastern Europe, communication expert, and media analyst, in an interview for this study.[20] This is a significant message that positions the President of Ukraine as a leader striving to secure his place in history as the individual who definitively ended Russia's ambitions toward Ukraine.

Here, we arrive at another dimension targeted by President Zelenskyy's communication: building a personal and national "brand". Zelenskyy is widely regarded today as a politician who has established his "brand" on the international stage. In this regard, Ditmir Bushati states, "There is no question that Zelenskyy is a kind of political 'brand' and a model for the democratic world, as well as for those who believe in the values of freedom." Adam Richardt shares this view, arguing that Ukraine has cultivated a political brand as a nation united in its defense against aggression and its struggle for freedom and survival.

The deliberate involvement of Olena Zelenskyy, wife of the Ukrainian President.

The battle for public attention has spared even the wife of the President of Ukraine. Olena Zelenskyy has been "fighting" on the front lines since the early weeks of the war. Her intentional involvement underscores the importance that President Zelenskyy places on public communication. The role and impact of the First Lady in international public relations have been so significant that she has sometimes been

[19] Interview with Ditmir Bushati.

[20] The interview was conducted on May 29, 2023.

described as "Ukraine's secret weapon.[21] Public relations require originality and emotional appeal to create the desired impact. In this context, Olena Zelenskyy's involvement in international public communication is designed to evoke the strongest human emotions.

Ukraine is confronting Russia "militarily", a front known as "hard power," while simultaneously developing "soft power" through an aggressive public diplomacy agenda. This involves the communication of state and non-state actors, non-governmental organizations, corporations, and individuals with foreign audiences, aiming to inform, influence, and engage them in achieving the country's political and economic objectives"[22]

Findings

This study supports the hypothesis that "An elected leader, as a product of influence from traditional media (a serial film actor), is now building his successful international image through the development of social media".

Zelenskyy skillfully leverages the advantages of:

- The online world, through which he communicates with the parliaments of various countries, international organizations, the academic community, the business world, and others.

- Social media platforms, through which he engages with specific audiences.

- Video distribution platforms, through which he delivers messages in the language of the target audience.

The President of Ukraine has undertaken an "aggressive" international public communication agenda. He has utilized every platform, meeting, and opportunity to discuss the situation in Ukraine and call for assistance. Zelenskyy's communication focuses on several key themes, such as: resistance, victimization, the moral divide between good and evil, freedoms and rights, as well as virtues like bravery, justice, and others. He also emphasizes broader societal values, such as honor, glory, and fear.

His messages are directed to the audience as a whole, but in a targeted manner, he communicates with:

The international community,

The people and the military of Ukraine,

Putin and the Russian military, especially the Russian people.

[21] Peter Dickinson, 2022. *Atlantic Counse*l. July 28. Accessed April 8, 2023. Electronic resource: https://www.atlanticcouncil.org/blogs/ukrainealert/vogue-diplomacy-first-lady-olena-zelenska-is-ukraines-secret-weapon/.

[22] Hasan Saliu, Komunikimi ne Diplomacine Publike, Prishtina: AAB University College, 2015.

Zelenskyy is working to shape his historical image. His rhetoric has evolved over time. As early as April 2022, and continuing thereafter, Zelenskyy shifted from asking for peace to calling for victory in the war with Russia. Additionally, there was a clear division of roles between the two spouses.

"The President focuses more on the political message of the war, emphasizing the need for support and endorsement, as well as the motivating force for the military. In contrast, the First Lady centers her narrative on the human pain and loss that the nation of Ukraine is enduring. The image of women has always held significant influence in the Western world. Olena Zelenskyy addresses the international public both as a woman and as a mother.

Both spouses have chosen to communicate through their clothing, symbols, and silent messages.

Bibliography:

1. Zyhdi Dervishi, *Lente të ndërveprimit simbolik:analizë sociologjike e rolit të simboleve kulturore, të komunikimit joverbal*. Tirana: Ermal. 2016.
2. Manuel Castells, *Communication Power*. New York: Oxford University Press, 2009.
3. Alban Tartari, *Marrëdhëniet me Publikun.* Tirana: Luis Print, 2021.
4. Sinan Aral, *The Hype Machine*. New York: Penguin Random House LLC., 2020.
5. Olga Onuch & Henry E. Hale, *The Zelenskyy Effect,* United Kingdom: Hurst&Company, London, 2022.
6. Manuel Castells, *Communication Powe*r, Oxford: Oxford University Press Inc., 2009.
7. Volodymyr Zelenskyy, *A message from Ukraine*, London: Hutchinson Heinemann, Penguin Random House UK, 2022.
8. Artan Fuga, Mediamorfozë dhe Metakomunikim, Tirana: Papirus, 2017.
9. Peter Dickinson, 2022. *Atlantic Counsel*. July 28. Accessed April 8, 2023. Electronic resource: https://www.atlanticcouncil.org/blogs/ukrainealert/vogue-diplomacy-first-lady-olena-zelenska-is-ukraines-secret-weapon/.
10. Hasan Saliu, *Komunikimi në Diplomacinë Publike*, Prishtina: AAB University College, 2015.

Armed Force as a form of institutional violence. A theoretical approach based on liberal democratic countries

Lieutenant Colonel Latif SHURDHI
Lecturer at the Defense and Security College, AAF

Abstract

In this paper, the armed force is treated as a form of institutional violence that can be used to reinforce authority, to strengthen national security, or to calm or bring under control violent internal outbreaks. Naturally, its use may also have negative consequences in society, including violations of human rights and the escalation of conflicts. It is important that the institution responsible for the use of force, as well as the individuals entrusted with functional duties within such institutions, be careful in exercising this function, respecting national and international legality.

To create clarity for the reader we need to provide a definition of what the armed forces are. The armed forces, looking at them in the social sense of the concept from the numerical point of view of its members, are an organization and from the perspective of the norms and values they represent, they are an institution. An institution is an establishment of interconnected norms and roles that regulate a particular area of social life[1]*. As for the definition of the concept of "violence" and the connection of this concept with the institution of the armed forces, which is also subordinated in the form of an instrument in relation to the state, we will address this further in the discussion below. Additionally, we will explore the interconnection of various concepts with the armed forces, as well as their features and characteristics, which in sociology are important for making distinctions between concepts and their definitions. In a very concise manner, this article presents the armed force as a form of institutional violence; state violence and social practice; social practice within the armed force; the hierarchy and its importance for this institution; the military personnel with its characteristics; as well as some conclusions and perspectives regarding the armed forces.*

Keywords: armed force, *homo militaris*, military personnel, institutional violence, hierarchy, etc.

[1] Latif Shurdhi, *The Armed Forces and the family as "greedy institutions"*. Military Journal, no. 2/2014, Tirana, August 2014, p.130.

1. Homo Militaris, a Form of Institutional Violence

The Armed Forces represent a social field and a political institution[2], that organizes violence (the exercise of force) against other countries, defends the nation from external violence, and keeps means ready for the protection of internal order according to the need and legal conditions. In this institution, there is an integration of the tension between the vertical rationality of bureaucracy and the entire horizontal professional community. The military corporatist character is composed of the mechanisms of bureaucratic logic and the implied references to aristocratic-martial values and virtues.

Due to the specific merging of the dominant organization and the military profession, the armed force can be characterized as a corporation of violence. Military violence is a "collective good" provided by the armed force, which, for this reason, differs from civil society. The features outlined here describe the framework conditions within which the forms of social practice in the military field are formed, in which violence (according to Max Weber) and military culture in the sense of social practice (according to Pierre Bourdieu) are produced and reproduced. Therefore, the framework for the sociological analysis of this goes beyond the armed force as an organization and includes society as a whole, because social structures and organizations are understood in the same way as the armed force- as rational-purpose instruments for the realization of functional objectives, while they also present systems of symbols or meanings.[3].

2. State Violence and Social Practice

Since the 1960s, Renate Mayntz has pointed out that the rational organizational model of classical sociology has overlooked the *Weberian* context of sociology of power and bureaucratic treatment, and thus failed to distinguish that *Max Weber* understands bureaucracy and power as two principles that are always in tension with each other.[4] From here, it becomes clear that organizations must initially be understood as fields of social forces, in which competition takes place for the realization of various and sometimes opposing goals. Organizational structures are formed by both direct and implied rules, as well as by the distribution of economic, social, cultural, and symbolic capital in the context of *Bourdieu*'s theories. These types of capital represent an instance of social power and serve as the basis for legitimating power.

The Armed Force, as a tool for the external and internal self-exposure of the state, is a political institution on one hand and a clear form of institutionalized violence on

[2] Grhard Goehler, *Institutionenlehre und Institutionentheorie in der deutschen Politikwissenschaft nach 1945*: *Grundfragen der Theorie politischer Institutionen. Forschungsstand, Probleme, Presprektiven*, Opladen 1987.

[3] Ulrich vom Hagen, *Homo Militaris. Prespektiven einer kritischen Militärsoziologie*, Bilelefeld 2011.

[4] Renate Mayntz, *Soziologie der Organizationen*, Reinbek, p. 32.

the other. The Armed Force is under the state control, which *Weber* understands as an organization that holds power, because every state, as a coercive (mandatory) institution, is based on violence and physical violence, as a specific tool, is its monopoly[5]. The Armed Force and its principles are closely linked to the state. The main question posed here is: which structures allow the commands of the leader to be executed with the least possible losses caused by friction within the apparatus? According to *Weber*, the only system that would fit this requirement is the modern rational bureaucracy, which in its purest form represents a system of goal-rational actions interconnected with each other, and for the emergence and unfolding of which, among other things, a condition is presented: the concentration of material resources in the hands of the employer.

Thus, the historical bureaucratization of the armed force is fundamental to understanding it as a political instrument of state violence. The concept of institutional violence integrates both actual and potential violence (*according to Weber*), as well as symbolic violence (*according to Bourdieu*), and is defined by the sociologist *Peter Waldman* as follows: "The concept of institutional violence (...) in this sense goes beyond the personal, direct meaning of violence. It does not focus only on the specific modalities of social activity, but also on ongoing relationships of dependence and persuasion. Violence can be defined as a power exercised through physical sanctions, which is granted to those in hierarchical positions over their subordinates. (…) A prototype of institutional violence in modern times is the demand for recognition and obedience with which the state confronts the individual"[6].

Therefore, we can affirm that institutional violence summarizes state violence. So the characteristics of the monopoly of violence and state violence, like those of the armed force, are the form of institutional violence and its culture.

3. Social Practice in the Armed Forces

In order to define the culture of the armed forces, it is necessary to break away from the often-assumed homogeneity of it and pose the question of what it truly involves within its field. Therefore, the question arises about the definition of the essence of the armed force of a country, and depending on the acceptance of this perception, the chances within a military career. In the spirit of the corps, cohesion is simultaneously expressed, but also the conformity of those who have already managed to find acceptance in the social world of the armed forces. These mechanisms constitute the "corporate" character of the armed forces. Additionally, within the armed force, subcultures can be found, especially among the main component forces (land, naval, and air forces), among the special branches of the land forces, or in the form of rank groups (officer, non-commissioned officer, soldier), as well as through the distinction between troops at home and those on overseas missions.

[5] Max Weber, *Wirtschaft und Gesellschaft. Grundriss der verstehenden Soziologie*, Tübingen, 1972 (1921).
[6] Peter Waldmann, *Politik und Gewalt*: *Dietr Nohlen/Reiner-Olaf Schulze (Hrsg), Lekxikon der Politik, Bd. 1: Politische Theorien*, München, 1995, p. 430.

The conflicts that arise between actors and specific groups in the social field are based on the specific antagonism of the field in relation to the opportunities for exploiting social, cultural, symbolic, and economic capital. Therefore, it is helpful to view the armed force, like other fields, as a field of play, in which there is competition for the power of interpretation and this generates a certain habitus, which allows for a self-evident and natural adaptation to the rules of the specific field's game.

As part of the state apparatus, the armed force holds extreme significance for the political sphere because the state apparatus stabilizes the social relations of power. Based on *Max Weber's* well-known definition, the state possesses the monopoly of legitimate symbolic power over individuals living within its territory. The legitimacy of this monopoly on power, both domestically and internationally, is achieved through the armed force. The armed force integrates the political representation of the unity of the people, territory, and state in a unique way, granting them a special regulatory and protective role[7]. Through the representation of this trinity, the armed force legitimizes the state and, ultimately, itself.

Bureaucratic logic on one hand, and at the same time the reference to military virtues and leadership on the other, form the model of military order. From these, a continuous tension arises within the armed force between modern reality, expressed in bureaucratic discipline aimed at conforming behavior to rules regardless of the personality of the leader, and pre-modern perceptions of the military leader's figure, which corresponds to the figure of the charismatic personality with its specific individual characteristics. The foundation of every military culture here forms the "historical model of the Prussian corps"[8], to which reference is made globally. Beyond this, military strategy and tactics, techniques, values, norms, and military virtues become tradition and are passed down. All military organizations have in common basic education and courses through which individuals are instilled with military culture in the form of a social process and are taught the military way of life. During this process, soldiers, among other things, are instructed in hierarchy, bureaucracy, rules, laws, military society, trust, loyalty, military symbols, rituals, and specific military vocabularies, and thus the culture of military discipline is absorbed and adapted, which exists in all military organizations.[9] Through multinational joint military missions abroad and encounters with military personnel from different armed forces, the historical continuity of the foundation of military culture is better guaranteed than ever.

Military culture is reflected in the activity of the military, which is found in the rules and regularity of this sociological field. Soldiers are instructed during basic training

[7] Klaus Ender, *Multikulturalität als Dilemma* at: Remi Hess/Christoph Wulf (Hrsg) *Grengänge.* Über *den Eignen und dem Fremden*, Frankfurt am Mai, New York 1999, p. 44.

[8] Eyal Ben-Ari/Efrat Elron, *Blue Helmets and White Armor: Multi-nationalism and Multi-culturalism among UN Peacekeeping Forces.* Armed Forces &Society, 2 (2001) p. 284.

[9] Joseph Soeters/Donna Winslow/Alise Weibull, *Military Culture.* Guiseppe Caforio (Hrsg) *Handbook of the Sociology of the Military*, London 2003, p. 250.

and during their military service in specific military principles, which include, among other things, obedience and techniques for wounding and killing. During this formative process, they are educated with military values such as discipline, loyalty, courage, sacrifice, and selflessness. In addition to this, a central role is played by masculinity, the sense of common belonging, and behavior in accordance with the rules. In this way, soldiers unite around a specific interest in their struggle for the object of that interest, which they believe in and possess.[10] Hierarchy and collective sentiment crystallize as the main shared elements, which are of central importance in determining the armed forces and their unique culture. Within the tension between these two elements, there are other forms that are important for both social and military practice. The practical forms of the military field are divided into two basic dimensions (hierarchy and collective), each with three elements: (discipline, formalism, and conservatism; segregation (grouping), manhood (masculinity), tradition and convention).

4. Hierarchy

The armed force, as a social organization, fundamentally consist of a large number of fighters, but initially, through its strong integration into the state in the 17th and 18th centuries, the condition for hierarchy emerged, allowing the transition from armed groups (territorial) to a formal, ready-to-act armed force. In the 19th century, the armed forces developed further, transforming into a larger, more formal state organization. Violence or state force is manifested, among other things, through the armed force, and it can be used not only in external relations but also for combating internal unrest, depending on the legal situation. Because the armed force, as the bearer of the monopoly on state violence, continuously present a risk to political leadership, the executive gives great importance to the absorption and consistent implementation of the principle of primacy of politics within the armed forces. This is achieved by installing the principles of command and obedience at all levels of the armed force. Command and obedience are central elements of the hierarchy within the armed forces, which, through discipline and state bureaucracy, teaches a form that means a formal definition of practices and competencies. As a large bureaucratic group, the armed force forms a distinct hierarchy, which is an expression of the authoritative structures that produce a clear chain of command and control. At the same time, the system of ranks and grades creates a social distance between military ranks, which not only correspond to competencies, but also to the manner of behavior that is appropriate for each rank.

The bureaucratic aspect of the military profession corresponds to the ideal type of the military planner (*managerial leader*), who exercises power in Weber's sense primarily through rational legitimacy [11]. In contrast, this stands opposite the ideal type of the military leader as a warrior (*heroic leader*), who legitimizes his power

[10] P. Bourdieu, *Sozialer Sinn. Kritik der theoretischen Vernunft* Frankfurt am Main, 1987, p. 124.

[11] Morris Janowitz, *The professional Soldier. A social and political portrait*. New York 1960.

through charisma and tradition. Keeping these two types of leaders in mind, the process of leadership in the armed force according to the restorative groups is understood primarily as a concept centered on the person. Here, the primacy of actions (the accomplishment of tasks) holds sway. The armed force, as a symbol of the unity of a people, territory, and state, also freely possess an attractive force for young people with conservative-national and radical right-wing political orientations because, as a result of the principle of command and obedience, discussions and freedom of conscience are considered non-military. Meanwhile, hierarchy and the principles linked to it, such as dependency and ranking within the military structure are seen as appropriate. The attitude and type of homo militaris correspond to the military fighter as he may be found in the armed force.

The circumstances for which soldiers must be prepared—to fulfill their duties even under the conditions of war—mean that the ideal image of the soldier is influenced by his duty to fight. Thus, this ideal type applies equally to all armies, regardless of the era or political system, and irrespective of what the official image of the profession of soldier in an armed force might suggest.

In a concept that considers the military leader as a generalist, which is the prevailing image for officers, various demands for "ideas and deeds" meet together. Here, there is a tension between modern rationality, functional discipline, and bureaucratic regularity on one hand, and on the other, the violent totality of the institutions of war, as well as the image of the soldier as a warrior. The military ethos, which consists of the traditional image of the soldier, stemming from the spectrum of conservative thought and from the military virtues of obedience, loyalty, discipline, courtesy, justice, honor, and willingness to sacrifice, conditions the military character.

It is precisely these orientations towards military values, principles, and virtues of readiness for sacrifice and selflessness that present the imagined model of action, perception, and thought that embodies the military character in relation to appropriate and successful action in the armed force. Thus, hierarchy in the military is defined both by *function* and by *leadership*.

5. Military personnel

Initially, in the armed force, the motto that the success of the group comes before the success of the individual holds true. Historically, in the conduct of war, the numerical superiority of forces has been emphasized on one hand, while on the other; the group is of great importance to the soldier because it provides security during war. In this context, the idea of the spirit of the group can refer to the unit or the sub-unit of the soldier (e.g., the company), but it can also be applicable within a group of soldiers of the same rank. Especially the corps of officers and non-commissioned officers, beyond each part of their affiliation with the force, is understood as a community with the same views in thought and action, because both are, at least until now, for two different social strata and different positions within the hierarchy. The officer

corps in Germany and other Western societies hardly recruits from the "desired"[12] strata anymore. They consisted in Germany, since the time of the empire from the strata of officer families, landowners, as well as from the "desired groups" of the educated bourgeoisie (from families of senior personnel, as well as from academic professions and liberal professions).

Due to the fact that the armed force, despite efforts to integrate women, remains a bastion of masculinity and a social space for the reproduction of masculinity, the perceptions of the "real" soldier's image are of a masculine character[13]. The human socialization of the soldier is evident, as the military is geographically separated from civil society[14].

The main idea expressed by the armed force about belonging in the military group is symbolically oriented toward a masculine society. In premises, which, until recently, were reserved exclusively for men, serious competitive activities are carried out according to male-coded rules. The collective society of a male grouping possesses the ability to ensure the preservation of the necessary unity during serious, concrete situations (e.g., during combat). The collective society also serves to shape gender differentiation.

The specific perceptions of appropriate behavior are closely linked to the right attitude. These are expressed, among other things, through the labels and norms of the collective, from which membership in a faction or subgroup within a group of equal rank originates. The traditional legitimation of power, according to Weber, is expressed through the mastery of appropriate styles and forms of behavior. These similarities with the contexts of civil situations help to overcome or conceal insecurity. Beyond this, the mandatory rules of behavior under the potential conditions of life separation and use in combat operations take on a functional significance. In this context, religious faith still plays a significant role in many armed forces across different countries. It is used especially when a death occurs. Traditional religious care in the daily life of the military does not have much significant value, but it still serves in the further transmission of specific military virtues.

The self-commitment of a professional corps to the specific values and norms envisioned for a state servant is materialized through state objectives and goals. The ethos of military service is expressed not only in the collective professional self-commitment to moral behavior for the good of the homeland, but also in the military oath, which sanctions the obligation to obedience and virtuous conduct. It remains to be ascertained whether in the armed force certain virtues have or are given greater

---

[12] Detlef Bald, *Deutsche Offizier. Sozial- und Bildungsgeschichte der deutschen Offizierkorps im 20. Jahrhundert*. München 1982, p. 41.

[13] Ruth Seifert, *Männlichkeitskonstruktionen: Das Militär als discursive Macht. Das Argumet*, 196, (1992), p.859-872.

[14] Jean Lipman-Blumen, *Toward a Homosocial Theory of Sex Roles. An Explanation of the Sex Segregation in Social Institutions*. Signs, 3 (1976), p. 15-31.

importance. Regarding the profile of the requirements of the military profession, *courage* may serve as a *primary military virtue*, because it inherently reflects the readiness for combat and self-sacrifice when required.[15] Bravery should be understood to some extent as steadfast courage, as well as the unwavering confrontation of threats and burdens. *Secondary military* virtues arise from further conditions that are linked to the soldier's duty. Depending on the position within the military hierarchy, *secondary functional virtues* such as discipline, determination, obedience, endurance, unity, sacrifice, courage, and judgment are given varying degrees of importance. These virtues essentially reflect the specific demands of military duties. *Secondary character virtues*, such as sincerity, persistence, simplicity, wisdom, maturity, honesty, calmness, self-sacrifice, loyalty, willpower, and dignity, possess or have high moral requirements. Secondary character virtues form the ethos of the military profession. Here, we are talking about a specific code of conduct, which enables a shared identification based on the same values.

The particular emphasis on these virtues in the military serves not only for collective self-description, but also helps to create and maintain the collective. They also provide the opportunity for soldiers to distinguish themselves from others, either consciously or unconsciously.

In the operational areas, models of behavior and social-cultural thought have been developed, as well as specific operational identities that have influenced the armed forces not only structurally, but also socio-culturally[16]. The separation of social premises, which, for the military is becoming more and more common in operations abroad, is taking on a new dimension, because the field camp in the area of operation is both a formal organization of the military and a place of residence for them. The boundary between the three activities- sleep, leisure time and work become blurred and often merges into one. At the same time, there are clear boundaries to civil society in the social and geographical context[17]. In the mission, there is not only a comprehensive separation of the camp site from the population of the operation area, but for each soldier, the mission also means separation from his family and private environment.

Conclusions and perspectives

The military field possesses specific elements, where, with the help of its characteristics, it can crystallize a culture of the armed force. These elements have been partly shaped by functional conditions and partly by historical developments. A perspective that stands out as a result of being closed off and, as it seems, being in collective unity, allows for the understanding and interpretation of the armed force as a heterogeneous collective within a society. The theoretical approach proposed

[15] Carl Amery, *Die kapitulation oder Deutscher Katholizismus heut.,* Reinbek 1963, p. 12.

[16] Ulrich vom Hagen/Maren Tomforde, *Militärische Kultur*: Nina Leonhardt/Ines-Jacqueline Werkner (Hrsg) "Militärische Sozioligie–Eine Einführung", Wiesbaden 2012.

[17] Donna Winslow, The *Canadian Airborne Regiment in Somalia: A Socio-cultural Inquiry.* Ottawa 1997

here for military culture focuses on the dominant social practices in the military. The valid perceptions of the "true" essence of the armed force are not only pursued by various military groups, but also the generations formed and absorbed there. Depending on the social strata from which recruits come to the armed force and how constant its duty remains, social practices within it change more slowly or more quickly. These social conditions are formed in military culture in a focused manner.

Through high moral demands, often carried outside the military society, which soldiers establish for their profession, the armed forces clearly appear as a *'moral organization'* in the sociological sense. The "*disinterested"* values of military society, with honor as its central axis, as observed from the tradition of this field, and the "*interested"*" values of civil society with a competitive character clash in this social sphere, lead to constant contradictions between military and civilian culture. In the bureaucratic armed force of a modern stratified society, it is difficult for anyone to act without interests or with honor according to the ideas of "military aristocracy". This makes the cultivation of formal practices of honor even more important. Despite the hierarchy in the armed force, in terms of professionalism and collegiality, there is talk of 'collective belonging.' Here, hierarchy and collective feeling are expressed simultaneously.

The ideal type of the soldier shows some variation from era to era and from country to country, but at its core, it remains constant and serves the armed force to maintain military principles of resilience, readiness for sacrifice, and a sense of collective belonging during the daily routine in peacetime.

The armed force, as part of state violence and as the central location of institutional violence, integrate the relationship between the conditions of power, force, and violence like no other political institution. Through the armed force, the existence of a violent organization is enabled, where the elementary experiences of combat, killing, and death are self-evident. Even during the daily routine in the bureaucratic military organization, the self-evidence of the orientation towards war is maintained through experiences of operations in missions abroad, through training, through direct normative requirements, as well as through the cultivation of the military tradition of the armed forces. As a political institution of the state and society, the armed force shapes both the soldier and the civilian, thus producing *the homo militaris, the military man."*

Bibliography:

1. Military Journal. Theoretical-Scientific Journal of the Training and Doctrine Command. No.2/2014. Tirana. August 2014.
2. Hantington, Samuel P., Ushtaraku dhe Shteti. Military Publishing House, Tirana. 1995.
3. Lufta, morali dhe profesioni ushtarak. Military Publishing House, Tirana. 1998.

4. Moskos, Charles C., From Institution to Occupation, “Military and Society”. Washington DC. 1974.
5. Janowitz, Morris. The professional Soldier. A social and political portrait. New York. 1960.
6. Goehler, Gerhard. Institutionslehre und Institutionentheorie in der deutschen Politikwissenschaft nach 1945. Grundfragen der Theorie politischer Institutionen. Forschungsstand, Probleme, Prespektiven. Opladen. 1987.
7. Von Hagen, Ulrich. Homo Militaris. Prespektiven einer kritischen Militärsoziologie. Bielefeld 2011.
8. Mayntz, Renate. Soziologie der Organizationen. Reinbek. 1963.
9. Weber, Max. Wirtschaft und Gesellschaft. Grundriss der verstehenden Soziologie. Tübingen. 1972.
10. Waldmann, Peter. Politik und Gewalt. Lexikon der Politik. Bd.1. Politische Theorien. München. 1995.
11. Bourdieu, Pierre. Sozialer Sinn. Kritik der theoretischen Vernunft. Frankfurt am Main. 1987.
12. Bald, Detlef. Deutsche Offizier. Sozial und Bildungsgeschichte der deutschen Offizierkorps im 20. Jahrhundert. München. 1982.
13. Seifert, Ruth. Männlichkeitskonstruktionen: Das Militär als destruktiver Macht. Das Argument. 1992.
14. Lipman-Blumen, Jean. Toward a Homosocial Theory of Sex Roles. An Explanation of the Sex Segregation in Social Institutions. Signs,3 (1976).
15. Amery, Carl. Die Kapitulation oder Deutscher Katholizismus heute. Reinbek. 1963.
16. Winslow, Donna. The Canadian Airborne Regiment in Somalia: A Socio-cultural Inquary. Ottawa. 1997.
17. Von Hagen, Ulrich/Tomforde, Maren. Militärischer Kultur. Militärische Sozologie – Eine Einführung. Wiesbaden 2012.

FOURTH RUBRIC

HISTORICAL WRITINGS

Albania's military alliance during the Cold War

Colonel (R) Dr. Ahmet LEKA
Deputy Dean of the Faculty of Defense and Security, AAF

Abstract

The security, integrity, and empowerment of a country are ensured when the protection of national interests and values is effectively fulfilled in a timely manner and with a forward-looking perspective. A nation's history, origin, geostrategic position, culture, language, traditions, and unique characteristics all contribute to its significance in the international arena. These elements illustrate the role a country can play within the broader community of civilized and progressive peoples.

After the Second World War, Albania emerged as a fragile country in every aspect- economically, politically, and strategically. It was a small nation with a severely underdeveloped economy, lacking infrastructure, and, as such, held little external appeal. The state leadership deemed recognition by the communist bloc as a necessity for its country.

Despite the establishment of diplomatic relations between Albania and Bosnia and Herzegovina, Moscow's connections with Tirana, up until 1948, were mediated exclusively through Belgrade. This was one of the factors that intensified Yugoslav influence in Albania. At the time, Albania faced significant challenges in its relations with neighboring countries. The "Friendship" with Yugoslavia had begun to show serious cracks, while Greek guerrilla forces frequently appeared near Albania's borders, often provoking incidents. As a result, Albania found itself in the dangerous "crossfire" of its neighbors. Consequently, participation in a coalition like the such as the Warsaw Treaty, would render Albania even more protected and secured.

Keywords: Second World War, Yalta Conference, diplomatic relations, Russian influence, Cold War, Albania's geographical position, Albanian Military, national security

1. The Yalta Conference and Albania

Before the end of the Second World War, in February 1945, a meeting was held in Yalta, Crimea, between U.S.A. President Roosevelt[1], leader of the Soviet Union Stalin[2] and British Prime Minister Churchill[3]. At this conference, these three statesmen discussed the future course of the war. They first and foremost reaffirmed decision made at Teheran regarding the division of Germany and Poland, as well as the allocation of spheres of influence after the end of war.

At the Yalta Conference, there was no fixed order or formal agenda. Discussion points were neither prepared in advance nor thoroughly considered. The primary topic of discussion was Germany's capitulation. The Allied leaders agreed to defeat Nazism and fascism, contributing to the victory of "democracy". Ultimately, Churchill succeeded in securing an agreement for the German Empire to be annexed and placed under the administration of the victorious powers. The principle of dividing Germany into four occupation zones was also confirmed at Yalta.

Debates about Poland occupied a significant portion of the conference discussions. The Soviet Union was promised the eastern part of Poland, up to the Curzon Line. To compensate, Poland was to receive German territory along the Oder-Neisse line. This arrangement effectively made Poland a satellite state of Moscow, serving as a buffer against the West. At the same time, the Soviet Union had occupied a substantial portion of Eastern Europe, as well as parts of the Balkans. Consequently, hundreds of millions of Europeans were incorporated into the Soviet sphere of influence. Countries such as Poland, Czechoslovakia, Hungary, Romania, Bulgaria, Yugoslavia, and the eastern part of Germany were liberated by the Red Army. Albania, however, was liberated by its National Liberation Army, though this occurred as the Allied forces from both the East and the West delivered the final blow to Nazi Germany. Otherwise, it is uncertain how long the Nazi occupiers would have remained in control of our country.

In reality, after the Second World War, it was not the Albanians who determined which sphere of influence they would belong to. Instead, it was decided at Yalta, the conference of the three major Allied leaders, Stalin, Roosevelt, and Churchill. At this conference, Albania (though it was not even mentioned by name) was placed in the Soviet sphere of influence. The compromise in Yalta was not made in the form of a contract, but mostly in a declarative form. The fact that the USA and the Soviet Union interests were more important than those of Europe, cannot be undeniable.

---

[1] Franklin Delano Roosevelt (January 30 1882-April 12 1945) was President of the USA from 1933 to 1945.He drew up a clear program of reforms to get the country out of the crisis.

[2] Joseph or Josif Vissarionovich Stalin (1878 - 1953), (Dzhugashvili), was the leader of the Soviet Union from the mid-1920s until his death in 1953. He emerged victorious in World War II.

[3] Sir Winston Leonard Spencer Churchill (1874 - 1965) was a British statesman, politician, diplomat, soldier and writer who served twice as Prime Minister of the United Kingdom, from 1940 to 1945 during World War II World and again from 1951 to 1955.

What is truly surprising is that Albania was not even mentioned in the decisions made at the Yalta Conference in February 1945, just three months after the Albanian communists seized power, which they would hold by force for nearly 45 years. It is as if Albania did not exist at all! As we will explore further, Stalin seemed to have little knowledge of Albania, a country that had no historical ties to the Slavs. But how could Roosevelt and Churchill "forget" the nation President Woodrow Wilson had persistently defended Albania's territorial interests at the Versailles Peace Conference (1919-1920) stating: *"In Europe, there is a small country with an ancient history and traditions, as well as a rich culture. For 500 years, it was under the occupation of the Ottoman Empire, and yet it managed to preserve its language, unique among the Balkans and Europe, along with its traditions and culture..."*

This can be explained by the fact that it was a consequence of the "partition" of the zone of influence in Yalta that Churchill made with Stalin and, when talking about Yugoslavia, maybe Albania was considered part of Yugoslavia. It is another tragic truth that proves once again that Europe, even with regret, including this time America, did not pay attention to this country and this people, thus reminding us of Fishta's well-known verses[4], excerpted from "Lahuta e malcis" (The Highland Lute**)**: " *Europe, aging whore, it's you that*, / *On your word and God have trampled*, / *Is it sign of all your culture*, / *That you parcel out Albania*, / *Just to rear the cubs of Russia*?"[5]

Thus, just like the Congress of Berlin in 1878, where German Chancellor Bismarck denied the existence of the Albanian nation; a congress that, through its arbitrary decisions, severed entire northern territories from Albanian lands, such as Plav and Gucia, granting them to Montenegro, and handed Serbia other Albanian-populated areas in the regions of Vranje, Nish, and beyond, up to the outskirts of Gjilan; the same did the London Conference in 1913, which gifted Kosovo to Serbia. This time, the "three great powers" mentioned above acted even worse at Yalta, because, without any formal decision, they implicitly regarded Albania as part of Yugoslavia, effectively granting her the right that one day would even devour Albania...

At Yalta, it was decided between Churchill and Stalin that Romania and Bulgaria would be 80% under Soviet influence and 20% under Western influence. Yugoslavia was to be 50% under Soviet influence and 50% under Western influence. Greece was assigned 80% under Western influence and 20% under Soviet influence. "As for Albania, it was not specifically discussed, but, as it was clearly evident from later developments, it was included within the framework of Yugoslavia, which fell entirely under Russian influence."[6]

---

[4] Gjergj Fishta (October 23 1871-December 30 1940), was a Franciscan, educator, writer, translator, poet, playwright, prose writer, but also as a critic, literary historian and esthete, who for half a century was the dominant figure of Albanian literature, he was even crowned "national poet" while he was alive.

[5] Gjergj Fishta "Lahuta e malcis" (The Highland Lute**)**

[6] Ramiz Alia, *Jeta ime (My Life)*, page 136.

This, therefore, was the fate that befell Albania. What might have happened if the "three great powers" at Yalta had made a decision specifically for our country, ensuring that it was not crudely considered part of Yugoslavia—since it was not a Slavic country—but instead placing it 80% under Western influence and 20% under Soviet influence? Or perhaps deciding that Albania should be equally connected to both East and West, as non-communist forces that represented other political directions had also participated in this war?

2. Political blocks after the Second World War and Albania

As expected, the post-World War II resulted not only in winners and losers, but also in a deep division among the winners themselves. The Allies retreated to their trenches, no longer as allies, but as opponents. Two political and military blocs faced off in a new conflict, which, in historical and political terms, came to be known as the "Cold War", a term firstly used by the American journalist Walter Lipman.

After the Second World War, Albania was politically aligned with to the Soviet Union. Immediately after the war, from the Soviet Union's perspective, Albania was just a small country, with a completely backward economy, without any infrastructure and, as such, entirely unappealing. The Soviet Union's interest in Albania was primarily in the context of strategic military concerns, seeking to include it within its sphere of influence. Soviet support for Albania's issues at the United Nations had precisely this aim. Until 1948, regardless of the establishment of diplomatic relations between Albania and the Soviet Union, Moscow's connections with Tirana were carried out solely through Belgrade. This was one of the factors that intensified the growth of Yugoslav influence in Albania. Until 1948 Albania remained under Yugoslav influence. The "eternal friendship" with its northeastern neighbor lasted less than four years (1944–1948).

Albania entered the Soviet sphere of interest only after the Soviet-Yugoslav split. The truth is that rather than economically supporting Albania, the Yugoslavs saw it as a resource to exploit, appropriating leftover stockpiles of goods that had remained in Albania when Fascist Italy brought large supplies to Albania for its propaganda purposes.

On this matter, Petro Marko[7] recounts the complaint of a merchant from Shkodran in 1945, when he was the editor-in-chief of "Bashkimi"[8] newspaper, the only daily newspaper in the country: "Why, Mr. Petro, are the Slavs stripping us bare? At least let them take part of it and leave some for us—how are we supposed to find all these goods of every kind: from construction materials to textiles, machinery, drinks, even down to toilet brushes?" Stalin abandoned Yugoslavia after creating a buffer zone between the Soviet border and the West, signaling with his rejection of Yugoslavia that he had no expansionist ambitions but was focused solely on the security of the Soviet Union.

[7] Petro Marko (1913-1991) was an outstanding Albanian educator, publicist, poet, writer and prose writer.
[8] "Bashkimi" newspaper, directed by Petro Marko, 1945-1947.

The abandonment of Yugoslavia was actually an act of self-restraint by Moscow, and at the same time the Soviet Union reduced aid to a minimum until it stopped completely, blaming Tito's betrayal. Following Yugoslavia's abandonment, Stalin maintained Albania as an advanced outpost, something like Kaliningrad after the dissolution of the Soviet Union. This was also due to the fact that the Albanian leadership chose to side with Stalin in the conflict between him and Tito.

After the breakdown of the relations of the Soviet Union with Yugoslavia, the suffocating Yugoslav oversight of Albania came to an end, and the aid provided by the Soviet Union to Albania began to flow directly to. Thus, there was now a symmetry in Albania's relations with the Soviet Union, both on the politically and economically.

In American documents, there are a numerous record that testify to the opposite. The US government traditionally and consistently presented itself as supporter of Albania's independence and territorial integrity. For the Unite States, Albania held no strategic importance, but it remained significant in the context of its broader interests concerning Italy, Greece and Yugoslavia. According to the US, these states had conflicting interests in Albania, which required careful attention to prevent the aggravation of tensions that could disrupt the political status quo in the Balkans, potentially leading to a broader and uncontrollable conflict. It appears that the goal of the USA was to isolate this conflict as much as possible and to separate Albania from the communist bloc without triggering any international complications.

Thus, the years 1948-1960 can be considered normal years in Soviet-Albanian relations, understood within the framework of the abnormal alignment of Albania with the Soviet Union. However, it is interesting to note the fact that, while the Soviet-Albanian relations gained an economic dimension, apart from the political one, they lacked the military dimension, even though such a request was made by the communist leadership of the time.

With Stalin's death on March 5, 1953, no one knew what would happen in the Soviet Union aftewords. Stalin's death marked the beginning of liberalization in the politics of his successors, leading to significant changes in the internal and external conditions of the Soviet Union.

The new leaders distanced themselves from the Stalinist leadership methods and decided to implement changes aimed at correcting the mistakes occurred during Stalin's rule. Parallel to these developments, measures were taken against mass repression and there was a liberalization in the socialist states under the Soviet Union's influence (with the exception of Albania). This process which lasted until the end of 1955, brought many improvements in living conditions at that time.

Before reaching this period, with the end of the Second World War, the Soviet Union began establishing agreements with states within the its sphere of interest. When the Soviet Union opposed Germany's membership in NATO, it made an agreement

with the Eastern Bloc countries for full support and mutual defense. The Treaty of Friendship, Cooperation, and Mutual Assistance was signed on May 14, 1955, in Warsaw. The socialist forum included the following states: the Soviet Union, Poland, Czechoslovakia, East Germany (GDR), Romania, Hungary, Bulgaria, and Albania.

3. The Warsaw Pact, Albania's membership in this pact

With the establishment of popular democratic regimes within the BS's sphere of influence at the end of the Second World War, questions arose about how the national defense and security of these countries would be organized. "...In this context, the task of defending socialism was entrusted to the armed forces, guided by the Marxist-Leninist ideology. This military-ideological transformation laid to foundation for the creation of a multilateral alliance to oppose the West".[9] The Warsaw Pact was an alliance of the communist states of Europe, led by the Union of Soviet Socialist Republics, (USSR). It was signed on May 14, 1955 in Warsaw, with the goal of fostering friendship, cooperation and mutual assistance between its members: Albania, Bulgaria, the German Democratic Republic, Poland, Romania, the Union of Soviet Socialist Republics, the Socialist Republic of Czechoslovakia and Hungary. The pact obliged its members to consult on matters of common interest and to provide immediate military assistance in the event of an attack in Europe against one or more member states.

According to the treaty, all member states of the Warsaw Pact were considered equal, and the principle of non-interference in their internal affairs was upheld. The agreement was initially set of 20 years, with no provisions for withdrawal from the alliance. This method of resolving conflicts among states was seen as a mechanism with limited influence on the advisory policy, creating a distance between these states. The bilateral agreements between the Soviet Union and the Eastern Bloc countries from 1944 to 1947 played a significant role in establishing military cooperation.

The Warsaw Pact was developed as a political instrument in the hands of the USSR, as the leading power of the Eastern Bloc. The efforts of the insurgent Hungarian government I. Nagy[10], in October/November 1956, to withdraw Hungary's membership of the Warsaw Pact, were pivotal in prompting the march of Soviet troops into Hungary in November 1969. Communist reform efforts in Czechoslovakia in 1968 were perceived by the USSR not only as a deviation from the communist ideology, but also as a threat of keeping the League together.

[9] Etleva Smaçi, Albania in the Warsaw Treaty 1955-1968, (Monograph), year 2023, pg.11.

[10] Imre Nagy was a Hungarian communist politician who served as the Chairman of the Council of Ministers (de facto Prime Minister) of the Hungarian People's Republic from 1953 to 1955. In 1956 Nagy became the leader of the Hungarian Revolution of 1956 against the government supported by The Soviets, for which he was sentenced to death and executed two years later.

After the march of Soviet troops into Czechoslovakia, August 1968, Albania withdrew from the Warsaw Pact.

Unlike the strategy of the Organization of Transatlantic Nations, the Warsaw Pact did not publish any defense strategy against attacks. Various Western military circles argued that, based on its command leadership, organization, training, and armament, the Warsaw Pact operated under an offensive military strategy. Given the spatial deployment of Soviet troops and their constant state readiness, it can be said that the Warsaw Pact aimed to ensure preparedness for potential conflicts, without any specific preparations or maneuvers. The daily improvement of the Warsaw Pact's conventional and nuclear armament meant that they were ready for any type of potential warfare at the time. With this strategy, the Warsaw Pact pursued equality with the United States of America and conventional dominance in Europe. Likewise, in some Western European countries, it was believed that the armament, which exceeded the Warsaw Pact's self-defense needs, was also used to suppress the interests of Western Europe. Albania became a member of the Warsaw Pact in 1955, while on October 24, 1957, the Soviets were granted the Vlora naval base. Albania's nature and geographical position are often considered substantial component of its national identity and key factors for the image. Albania is internationally recognized and regarded an undiscovered, untapped natural gem. Albania's nature and its landscape form a symbiosis of unique identity values. Albania's extraordinarily favorable nature and location are positive objective components believed to be gifts from God.

The geographical position of Albania, represents in itself a highly significant geostrategic element. Situated at the crossroad of the shortest routes connecting the western Mediterranean to the Balkans and Asia Minor, it holds control of a very key strategic point, the Otranto channel. So, it provides an internal connection of the Balkans with the Adriatic Sea, as well as between Asia Minor with the Mediterranean region. Albania is traversed by two critical corridors: Corridor VIII and Corridor X. Corridor VIII corresponds to the ancient Via Egnatia, while Corridor X represents the northern corridor of Albania. These corridors play a vital role, underscoring Albania's favorable geographical position for strategic integration within the region and Europe. The roads associated with these corridors act as essential arteries due to their strategic importance. The political-military strategic perspective of a country generally relies on its geostrategic position, military capacities, defense resources, interaction with allies, response to potential adversaries and of course its weight in international relations.[11]

The climate is another highly favorable element, as Albania lies within the subtropical zone and is included in the Mediterranean climate. This is characterized by relatively short and mild winters, along with hot and dry summers. Our natural resources and beauties have the potential to attract both foreign and domestic investors fostering further development of tourism, bringing economic growth, as well as social and cultural development.

[11] Hans Morgenthau, *Politics among nations, The struggle for Power and Peace*, 5th Edition (New York: 1985).

"The Albania's inclusion in this Treaty and later the offer to build in Vlora a joint military base with the Soviets and other communist countries was not easy, as the Russian communist leadership (Stalin, Molotov, etc.) had opposed it, with the argument that, if Albania were attacked, the Soviet Union would have to fight for it".[12] The request from the Albanian state to be accepted in the Warsaw Treaty in 1955 and the provision of the Pashaliman Base (1957) were consistent efforts. This move aimed to address the anomaly that Albania was that Albania was the only communist country in Eastern Europe, allied with the Union Soviet, without hosting any Soviet military forces, a situation perceived as a significant security risk, at that time. On the other hand, "Soviet military strategists, wanted to exploit this anomaly in terms of the strategic advantage that Albania provided. The Pashaliman military base was seen as one of the most adequate bases for bringing the Black Sea fleet closer to the Albanian coast to destroy the 6th American fleet".[13]

As mentioned above, Stalin opposed this idea, in both cases: when it was presented to him by the Albanian leadership in the years 1949-1952, and when it was proposed by the Soviet generals, with the argument that defending Albania would be a futile strategic adventure. This was because Albania was not bordered by other Warsaw Treaty member countries being separated from them by two countries allied with USA, Greece and Yugoslavia. In the event of a tense situation, when Turkey would certainly close the Dardanelles while Spain Gibraltar, using vain pretexts, but in reality, to prevent the Soviet fleet from entering the Mediterranean, the Soviet Union would not be able to supply Albania and its forces there with weapons and other necessary items. Therefore, Stalin still saw Albania as a bargaining chip with the West, which he could give up in exchange for something else. On the other hand, it should be noted that Stalin was not inclined to multilateral cooperation. He preferred loyalty in bilateral relations in all fields, including military ones. "Moscow preferred to be open and have a relation with each individual client rather than in a group"[14].

Soviet-Albanian military relations significantly strengthened in April 1957, when the Soviet Union gained access to Sazan Island as a military base. Despite its relatively small size of 5.5 square kilometers, the island's strategic location at the entrance to the Strait of Otranto only 5 kilometers from the Albanian coast and 65 kilometers from the nearest point in Italy made it highly valuable. This act, formally signed in October during Defense Minister Zhukov's visit to Albania, authorized the deployment of the Russian military fleet at the Vlora base. Albania was strategically crucial for the defense of the communist camp**.** However, the Dardanelles, the Bosphorus, and the numerous Greek islands presented formidable obstacles for the Black Sea Fleet. While the Soviet Union claimed it did not need excessive armaments, the defense of Albania was deemed as important as the defense of any Soviet territory. If Sevastopol held strategic importance, Vlora's fortifications would take precedence over Sevastopol's.

[12] APS Central Archive, fund 14, list 1, file 24.

[13] Right there.

[14] Wolker Laker, Europe in our time 1945-1952, Tirana: Dituria, 1996.

The request for Sazan Island was not unprecedented. Its designation as an international military base for the socialist camp had previously been proposed but rejected. Following the renewed Soviet-Yugoslav relations and the significant political shifts accompanying Khrushchev's rise to power, Albania received preferential status from the Soviet Union. The Bay of Vlora, along with Sazan Island, represented a crucial military and political fulcrum, influencing the delicate balance of power in the Balkan region.

The Soviet leadership prioritized establishing this military base to bolster both its military security and international prestige. This action was undertaken within the framework of the Warsaw Pact agreements. Conversely, granting the Soviet Union military access at Pashaliman was deeply provocative, violating Albanian sovereignty and undermining the interests of neighboring nations and the West. The subsequent deployment of the Soviet fleet to Vlora caused considerable alarm in the West, leading Khrushchev to withdraw the fleet. This strategic retreat was cleverly used as leverage in negotiations with the West regarding Berlin, simultaneously offering the West evidence of the Soviet Union's detachment from Albania. "The avoidance of open conflict, considering the presence of the Sixth American Fleet in the region where NATO had stationed, was achieved through careful measures outlined in the agreement".[15] Notably, the deterioration of the relations between the Soviet Union and Albania was a *deja vu* of the earlier rift between the Soviets and Yugoslavia, where the Soviets initiated the split while conveniently shifting the blame to the other side. Newly Accessible archives in Eastern and Central Europe, along with declassified CIA documents, have been instrumental in revealing that Albania's involvement with and eventual exit from the Warsaw Pact was not solely of its own making.[16]

Albania's relationship with the Warsaw Pact between 1961 and 1968 remained ambivalent, it was neither fully integrated nor entirely independent. The agreements of 1957 and 1959, and Khrushchev's visit, failed to enhance Albania's standing within the Soviet bloc or the Warsaw Pact. A CIA analysis even indicated that Khrushchev's visit ended two days earlier than scheduled.

On March 28-29, 1961, the Political Consultative Committee (PCC) of the Warsaw Pact convened in Moscow. This meeting attended by high-ranking officials including first secretaries of central committees, heads of councils of ministers, foreign ministers, defense ministers, representatives of state planning committees, and the commander-in-chief of the United Armed Forces. Khrushchev himself issued the meeting notice. In response to the Central Committee of the Party of Labor of Albania regarding the meeting's approved date and location, it was regretfully stated that both Enver Hoxha and Mehmet Shehu were unable to attend due to "health reasons". Enver Hoxha later characterized this situation in his memoirs as a "diplomatic illness". After facing severe criticism in Moscow from the leaders of the communist and labor parties, Enver Hoxha chose not to confront the critiques from his counterparts in the Warsaw Pact.

[15] AQFA, fund 100/1, V.1957, D23, fl3, Agreement no. 39.

[16] Etleva Smaçi, *Albania in the Warsaw Treaty 1955-1968,* (Monograph), year 2023, pg.7.

Minister of Defense Beqir Balluku would lead the Albanian delegation in Moscow. As anticipated, the meeting's tension was palpable. On March 22, 1961, at the Political Consultative Committee (PCC) of the Warsaw Pact, an Albanian document of 24 pages and a Soviet document of 6 pages concerning the incidents at the Vlora Base were submitted. The commander of the United Command, Greçko, definitely requested the Albanian government ensure the following: "If the intention is to maintain the presence of Soviet submarines and other warships at the Vlora Base, these vessels must be operated exclusively by Soviet crews. If this is not the case, the issue should be reported to the Political Consultative Committee (PCC) and presented to the Soviet government for consideration regarding the withdrawal of all Soviet warships, military personnel, and specialists from Albania". Beqir Balluku, in his speech, emphasized that "the liquidation of the Vlora base is not only in direct contradiction with existing agreements, but it also constitutes an impermissible violation of the sovereignty of the Republic of Albania. This action represents a direct infringement of the Marxist-Leninist principles that govern relations among the states of the socialist camp and the Warsaw Pact".

4. The Alleged Attack on Albania?

At the 4th Congress of the Party of Labor of Albania (PLA), Enver Hoxha[17]announced an imminent attack on Albania, allegedly orchestrated by the U.S. Sixth Fleet in collaboration with the Greeks, Yugoslavs, and traitors from within the country. The subsequent meeting of the Warsaw Pact's Political Consultative Committee (PCC) on March 28-29, 1961, revealed significant concern among participants, including Khrushchev, Kadari, Ulbrihti, Gomułka, and Dezhnev, regarding the Albanian leadership's claim of an "attack against Albania"' which caused unnecessary panic. Todor Zhivkov, First Secretary of the Bulgarian Communist Party, criticized the Albanian leadership's stance as "adventurous", urging them to focus on internal issues rather than engaging in provocative pronouncements. He also pointed out that "Albanian comrades", rather than "teaching us" Marxism-Leninism, should critically assess the leadership of their party and state. Identifying the factors that led them to this point and uncovering the "Albanian Beria" is crucial.

The Political Consultative Committee meeting concluded with a decision emphasizing that Soviet warships stationed in the Bay of Vlora would be crewed and operated exclusively by Soviet personnel, under the command of a unified Soviet command, which would be subordinated to the supreme commander of the armed forces of the member states of the Warsaw Pact. If Albania does not accept this measure, the Warsaw Pact members will be compelled to agree to the proposal for the withdrawal of the aforementioned military and naval forces from Albania. Furthermore, the Albanian government was urged to fully explain Enver Hoxha's statement at the 4th Congress of the Party of Labor of Albania, in accordance with Articles 3 and 5 of the

[17] Enver Hoxha (October 16, 1908 – April 11, 1985) was an Albanian communist politician and leader who ruled as dictator of Albania from 1944 until his death in 1985.

Warsaw Pact, concerning the so-called "attack on Albania". This request was viewed by many as a pretext to hinder rather than support Albania's continued participation in the Pact. In a series of letters addressed to the governments of Warsaw Pact member states, the Albanian government declared that it would under no circumstances hand over the naval military base in Vlora to Soviet crews. Furthermore, if the Soviet government decided to withdraw its military forces from the base, the Albanian government would not impose any obstacles. According to Enver Hoxha, under the current circumstances, the base no longer held any significance, and he argued that Khrushchev might exploit its presence as a pretext for deploying Soviet troops into Albania. Concurrently, the Albanian leader Enver Hoxha took serious measures to request military aid from China, while the Political Bureau issued directives urging that "the people should be made clear that, in the event of hard times, even war, they would need to tighten their belts and eat rationed bread" A month later, in November 1961, Enver Hoxha would directly address the Albanian people in a pathetic speech, declaring, among other things that: "We tell Khrushchev that the Albanian people and their Party of Labor will even eat grass, and we will not violate the principles of Marxism-Leninism." Thus, the communist leadership was leading Albania toward isolation, militarization, and extreme poverty.

5. Albania's Withdrawal from the Warsaw Pact

The Albanian military never participated in Warsaw Pact maneuvers. From 1960 onwards, Albania boycotted all Pact activities and meetings and formally announced its withdrawal from the Warsaw Pact after Warsaw Pact forces invaded Czechoslovakia on September 12, 1968. On May 26, 1961, eight submarines and one cruiser, crewed by Soviet personnel, departed from Vlora Base, involving the destruction and seizure of equipment at the Vlora base, further aggravated the situation. Ramiz Alia, leading the Albanian delegation at the Political Consultative Committee meeting held on August 3-4, 1961, was excluded from the proceedings due to the meeting's high-level nature, which stipulated participation only for First Secretaries. Khrushchev's public call in October 1961 at the XXII Congress of the Soviet Communist Party for the overthrow of the Albanian leadership signaled the complete breakdown of relations. The Albanian government responded by banning all Soviet broadcasts in Albania. Following this decision, mutual accusations between the two countries became so serious and frequent that it was hard to believe they had once been allies. On December 3, 1961, for the third time, the Soviet government sent a verbal note to the Albanian government regarding the removal of Albanian embassy staff in Moscow. By 1962, representatives of the Warsaw Pact had left Tirana. Albania's non-participation in subsequent Warsaw Pact meetings became evident when invitations were ignored. Nikita Khrushchev and other Soviet leaders accused the Albanian leaders of effectively excluding their country from the Warsaw Pact. The Polish government extended an invitation for a meeting of the Pact's Political Consultative Committee (CPC) in Warsaw on January 19, 1965, but the Albanian leadership publicly rejected it. A year later, the Albanian government sent a letter

to the Political Consultative Committee of the Warsaw Pact, expressing its concern about not being invited to the Committee meeting held in Bucharest from June 4 to 6, 1966. This *de jure* situation of Albania being part of the Warsaw Pact while de facto being excluded continued until September 1968. When the troops of the Warsaw Pact invaded Czechoslovakia, the Albanian government publicly denounced the action. On September 5, 1968, at the 5th Plenary of the Central Committee of the Party of Labor of Albania, Enver Hoxha drew this conclusion regarding the existence or non-existence of Albania in the Warsaw Pact: "The Warsaw Treaty did not provide adequate protection for our country; instead, it continues to pose a threat even after its revocation. By revoking the Warsaw Treaty, NATO countries can no longer justify an attack on Albania by claiming it is a member of that Pact. Instead, they will target a country that is not part of the Warsaw Pact, effectively eliminating that rationale." The Warsaw Treaty functioned as both a political and military structure, addressing the dynamics between the Atlantic alliance and the commitments of the participating countries. From today's perspective, this role is generally seen as regressive, often serving as an interventionist tool whenever governments fail to align with Soviet political leadership.

On June 4, 1961, the Soviet Military Fleet, following a series of conflicts between the Communist Party of Albania and the Communist Party of the Soviet Union, was compelled to abandon the most strategically important naval base in the Mediterranean, that of Pashalimani. Along with this advanced contingent, they were forced to leave in the hands of the Albanian military a modern arsenal of the time, which consisted of 4 submarines, the floating base "Nemcinov" 10 small vessels, 22 support ships, and a large number of weapons and materials, which the Soviet side classified as having been seized by the Albanian army.

When the Soviets abandoned the base, they discreetly removed essential logistical equipment, preventing the local forces from utilizing the equipment they had previously seized for combat operations. Furthermore, officers from that period have reported instances of former colleagues undermining their efforts by stealing torpedo detonators. Despite their small size, these detonators are critical components for the detonation of torpedoes and combat firing.

The torpedo serves as the primary weapon that endows a submarine with its combat capability. Each of our submarines was outfitted with 12 combat torpedoes: 4 located in the bow, 2 in the stern, and an additional 6 stored as reserves in the bow. A submarine typically carried approximately 100 detonators, including those within the combat reserve. Following the comprehensive control of these vessels, it was revealed that, in addition to various other damages, the detonators had also been stolen. Following the breakdown in relations with the Soviet Union, Albania's support from China remained the cornerstone of its international standing. Until 1978, China was the sole country from which Albania received military assistance. The Albanian government dispatched military missions to China to procure military equipment necessary for restoring the combat readiness of its forces. After 1978,

perceiving all neighboring countries as "enemies," Albania became entirely reliant on its resources for development.

The tense situation and the history of those days are well known, as the powerful tools of totalitarian propaganda elevated these conflicts to their peak. Military analysts regard this event as one of the greatest strategic losses for the USSR after World War II. The fall of the Berlin Wall in October 1989 brought significant changes to the established political balance and raised questions about transformations within the North Atlantic Alliance. It also prompted a reevaluation of the Alliance's relations with potential partners outside of it under the new circumstances.

At the Rome Summit in November 1991, NATO adopted a New Strategic Concept and took a significant step toward establishing formal cooperation in security and political matters between the Atlantic Alliance and the countries of the former Warsaw Pact. This was achieved through the creation of a new consultative body called the North Atlantic Cooperation Council (NACC). Albania became a member of NACC in June 1992.

Albania is bordered to the north by Montenegro and Kosovo, to the east by North Macedonia, to the south by Greece, and has a coastline along Italy. This geographic position makes Albania a pivotal country in the region, as many of its neighboring countries were once part of its territory. This historical context motivates Albania to promote stability and peace in the area, as it does not harbor hostility or make territorial claims through the use of force. Albania opposes the creation of crises and regional conflicts, consistently demonstrating this stance, especially during the recent upheavals following the breakup of the former Yugoslavia.

The environment and natural resources are vital components of a nation's development, and Albania is endowed with abundant underground minerals. These resources serve as significant instruments of national security, interest, and strategy. Additionally, our country's ancient civilization represents a substantial tourist asset. This rich heritage, shaped by a strong national spirit and millennia of tradition, exemplifies how a people can endure and thrive throughout history.

In today's world, significant global changes and resurgent nationalisms frequently influence the economic, financial, and military behavior of states or groups of states on the international stage. Therefore, it is essential for the Albanian political leadership to establish clear priorities and adopt a pragmatic and consensual approach to safeguard our key interests. Furthermore, engaging our nation and public opinion regarding our national values and interests is crucial, as it lays the groundwork for aligning the beliefs and ideas of both the leadership and the populace, thus enabling the optimal utilization of necessary capacities. Above all, it is important for Albanians to remember that neighboring states are also striving to assert their positions to advance their own security and national interests.

Albania is a pro-Atlantic nation that embodies the values associated with a Western orientation. Over the years of transition, it has demonstrated a strong commitment to

progress and development in alignment with the Euro-Atlantic model. Membership in Euro-Atlantic collective security structures have enhanced its awareness of effective strategies to bolster national security, thereby contributing to peace and stability in the region.

As a member of NATO, Albania is committed to its obligations as a genuine partner in security contributions and collaboration, providing support throughout the integration process into NATO.

Conclusions

- Throughout the Cold War, Albania was oriented in its ideological, political, military, and economic positioning on the side of countries with popular democracy.

- The concept of security and the strategic military dimension in their developments have been influenced by the ideological developments of the time.

- The Warsaw Treaty served more as a political-ideological instrument than a military one, where dictatorships were preserved and perpetuated through the armed forces.

- Albania had no role in the Warsaw Treaty, but it was simply a figurehead and a political maneuver and demagogic show only for the leadership.

- The base of Vlora was more like a political maneuver of the Soviet Union for expansion in facing the West.

- Albania's departure from the Warsaw Treaty was not at all a desire of hers, but a political bargain of the Soviet Union with the West, for certain interests.

Bibliography:

1. Erik Hobsbawm, *Age of Extremes*, Tirana, 1997.
2. Laker Wales, *Europe in our time, 1945-1992*, Tirana-1996.
3. Leon Poliakov, *Totalitarianism of the 20th century*, Tirana, 1987.
4. Henry Kissinger, *Diplomacy*, Tirana, 1999.
5. Karl Grimberg, *World History and Civilization*, Tirana, 2005.
6. Political and social studies, Tirana 1989.
7. Ramiz Alia, *My Life*, "About Albanian-Yugoslav-Soviet-Chinese relations (1944-1976)."
8. Kastriot Myftaraj, Journal "Panorama" *Soviet-Yugoslav and American-Greek parallels for Albania*.
9. Ana Lalaj, "Panorama" one of the most key moments in the history of Albania in the 50s.

NATO in the Western Balkans[1]: Albania's Journey from "Adversaries" to "Loyal Allies"

Prof. Assoc. Dr. Etleva SMAÇI
Lecturer at the Faculty of Security and Defense, AAF

Abstract

This paper aims to analyze the metamorphosis of the stance and role of NATO in the Western Balkans over the past three decades in comparison to its position and role during the Cold War. For this comparative analysis, the paper will explore the historical military context of the Cold War, with particular focus on the fact that most of the current NATO member states in the Western Balkans were once part of Yugoslavia, a country that followed a policy of "non-alignment with military alliances and blocs." The main argument this paper will present is that the disintegration of the former Yugoslavia in the 1990s, along with the shift in regime forms in certain states, urged NATO to change its position and engage in a region it had considered "out of area" for 40 years, specifically due to the widespread violation of human rights.

The second thesis of the paper will shed light on the regional implications resulting from the clash of NATO-Russia interests, following the shift in geostrategic balances in favor of the alliance. This thesis naturally raises the dilemma of whether NATO's involvement in the region will contribute to stability or if it will become a fertile ground for conflicts, precisely because of the historical past, during which the alliance itself followed the "hot potato" theory.

The last, but not the least thesis of the paper will focus on Albania's membership in NATO as a former member of the Warsaw Pact and with a communist legacy. The historical analysis of Albania's case will be closely linked to other member countries in the region, in order to explain whether we are witnessing the closure of the Cold War cycle in the Western Balkans or a modern version of it.

Keywords: Western Balkans, NATO, risks, security, Cold War.

[1] On this paper the term "Western Balkans" refers to 6 states: Albania, Serbia, Montenegro, North Macedonia, Bosnia-Herzegovina and Kosovo

Introduction

The North Atlantic Organization (NATO) was founded in 1949 with the clear goal of defending Western Europe from possible aggression by the Soviet Union and its allies. Although during the Cold War years the idea was created that NATO was outside the Balkans (while maintaining the areas of influence established at Yalta), in fact, the accession of Greece and Turkey in NATO and the creation of the Balkan Pact with the presence of Yugoslavia in 1953 gave a clearer idea of a careful presence in our region. With the fall of the communist regime in the countries of the socialist bloc in 1990-1991, the "threatening shadow" of Soviet aggression quickly dissolved. This was particularly helped by the dissolution of NATO's counterpart, the Warsaw Pact. Continuing with the idea above, NATO's presence was, in many circles, considered "excessive," as it had fulfilled its historical mission of protecting the West from communist ideology. Even less anticipated at the time of the fall of communism was NATO's ambition to fill the vacuum left throughout Central and Eastern Europe.

But these regime changes would confront the communist countries with new security challenges that could no longer be managed with the model of the "dictatorship of the proletariat." While the self-offering of the majority of Eastern and Central European countries to become part of a collective security organization like NATO[2] is entirely justifiable, the unknowns that have always demanded an answer are related to NATO's "renewal" in a region it had previously considered "out of area." And above all, the "approach" at a time when the "threat" of communism was no longer present, and the alibi of the Cold War had fallen.

From a historical perspective, referring to the documents adopted by the heads of state of NATO member countries in 1991, regarding what was considered the Alliance's new strategic concept, it can be stated that the "expansion of the border" was seen as the only way to preserve the "strategic balance in Europe."[3] On the other hand, if we refer to the preamble of the Washington Treaty, the member states of NATO do not base their unity solely on opposing communism, but primarily on shared values such as: the protection of freedom, democratic principles, the rule of law, etc. Consequently, this last argument was the key element that inspired the expansion strategy in the countries emerging from communism.[4]

---

[2] Strobe Talbott: *The Russia Hand*, The Random House Trade Paperback Edition, 2003, p:94.
Primary impetus for enlargement came from the presidents of three former Warsaw Pact countries. In April 1993, Lech Walesa of Poland, Vaclav Havel of the Czech Republic, and Arpad Goncz of Hungary appealed to Bill Clinton for the inclusion of their countries as members of NATO. Estonia made a similar request in May, arguing that it was crucial to prevent a future Russian re-occupation.

[3] North Atlantic Treaty Organization, "The Alliance's Strategic Concept," Agreed by the Heads of State and Government Participating in the meeting of the North Atlantic Council in Rome on 7-8 November 1991, paragraph. 21.

[4] "The North Atlantic Treaty Preamble," North Atlantic Treaty Organization, March 5, 2018, http://www.nato.int/cps/en/natohq/official_texts_17120.htm

As a result, since the Riga Summit in 2006, all countries in the Western Balkans had institutionalized their relations with NATO through the Partnership for Peace (PfP) or through the Euro-Atlantic Partnership Council. However, the 75th anniversary of NATO and the declassification of a number of documents previously unknown to the public this year have once again brought the attention of scholars to the question of whether this expansion, which included many of the former member countries of the Warsaw Pact as well as former Soviet republics, was justified or if, two decades later, it served as inspiration for Moscow's nationalist leader, Vladimir Putin, for a military revanche, such as the one against Ukraine?

If we consider the thesis that the expansion at the end of the 1990s and the beginning of the 21st century contributed to the "encouragement" of hostility with Russia, we must look retrospectively at some of the predictions made by prominent figures in international relations. Let us start with Henry Kissinger, who in January 1997 warned that "early in the new century, after many ups and downs, Russia is likely to have restored its central authority. This may be much closer to structures favored by Pinochet or Salazar than to Western pluralistic systems, although it would be freer than communism."[5]

The unpredictable future of Russia, which proved to be correct observation by Kissinger, led during the same period, Zbigniew Brzezinski and Anthony Lake to view expansion as the only way to maintain a strong Atlantic alliance. According to Brzezinski and Lake, the expansion of the alliance provided protection against the unlikely but very real possibility that Russia might revert to its past behavior.[6] This would be a very significant moment for the countries of Eastern Europe and the Western Balkans to become important regions for the Atlantic Alliance, while for NATO itself, it would mark an extraordinary turning point, as it would offer collective defense and security for those countries that, until recently, had been considered "enemies."

1. NATO and former Yugoslavia

In the 1990s, the Balkans region was often considered by NATO as a "headache."[7] Based on studies regarding NATO's relationship with the former communist countries of the region, the case of Yugoslavia was a very important test in the expansion challenge. Here, we will avoid analyzing NATO's humanitarian interventions, from its initial involvement with personnel of nearly 100 people in Bosnia and Herzegovina in 1992 to the case of Kosovo. The focus of this discussion is the analysis of the political and military factors that conditioned the accession of the former republics that emerged from the breakup of Yugoslavia into NATO.

[5] Henry Kissinger, A World We Have Not Known, *Newsweek*, 27 January 1997

[6] Zbigniew Brzezinski and Anthony Lake: "The Moral and Strategic Imperatives of NATO Enlargement". *International Herald Tribune*, 1 July 1997.

[7] Elena Zamfiresku, NATO and Balkans, *Perceptions Journal of International Affairs,* March-May 1999, Volume IV, Number 1.

The direct question is why the independent states created after the dissolution of Yugoslavia, such as Montenegro and North Macedonia, did not maintain the Titoist legacy of staying "out of blocs"? Such legacy continues to be "boasted" by Serbia, the legitimate successor of the former Yugoslavia, which officially has the status of a neutral state and is fully respected by the alliance.[8]

The new era of real politic and the geopolitical struggle that followed the end of the Cold War leaves no doubt about the thesis that the United States had—and still has—a highly ambitious plan for the Western Balkans and the new democracies in this region. The first step of this ambition could only be their inclusion in a collective security system (NATO), which they had created together with their allies immediately after the end of World War II. The purpose of this inclusion is clearly explained by Mr. Richard Holbrooke, linking it to the leadership role of the United States in Europe with "the creation of a security system that would stabilize all of Western Europe as well as the Soviet Union's satellites in Central Europe."[9] For Mr. Holbrooke, the expansion of NATO was nothing more than a consequence of the Iron Curtain that lasted for 45 years.[10]

But what was and remains the weakest point of the countries of the Balkans? The socialist state gave way to a capitalist state, based on a market economy and parliamentary democracy. This could be considered a "new order" for the Balkans, or in other words, an attempt to enhance democracy in a highly vulnerable environment. Therefore, NATO's "tasks" were not limited to what, during the Cold War, had been considered a military protective umbrella against aggression. On the contrary, the instability and political insecurity produced by the "newborn" democracies in the Balkans, which continue to be classified as hybrid regimes, have an impact on NATO's security zone. As a result, enlargement became mandatory, serving the stability interests of the organization's older members.

The post-1990 relationship between NATO and the Balkans is one of the most compelling illustrations of NATO's inherent capacity to adapt to new challenges. Although unwanted by anyone, the tragic history of the breakup of the former Yugoslavia and its subsequent consequences have, in a way acted as a catalyst for the adaptation of Alliances to the new challenges and risks of the post-Cold War era. On the other hand, NATO's adaptation has favored both its will and its ability to become an essential instrument for the gradual re-integration of the entire region into the mainstream of Europe. This enlargement was not only considered "healthy," but also led to the paraphrasing that if NATO did not move beyond the Cold War zone, it

[8] After Serbia's neutral policy, which is now surrounded by NATO member states, there are undoubtedly sufficient and clear reasons. First, one of the reasons for Serbia's distance from NATO is its close ties with Russia, traditional ties. Secondly, public opinion is one of the strongest opponents, stemming from the bombings of 1999 during the Kosovo war.

[9] Richard Holbrooke, *"America, A European Power",* Foreign Affairs, March/April l995, page 39.

[10] Ibid…. page 43.

would be out of business.[11] However, the concern was not about being out of business but rather about driving the first peacekeeping operations in the Western Balkans. On the contrary, the countries that joined the alliance learned lessons from their historical past that an expanding NATO was the only international organization that, with its integrated command structure and experience in joint allied exercises, was the right organization to carry out crisis management and peacekeeping operations beyond its borders—thus making regions of crisis like the Western Balkans suitable for use by other actors. It is worth noting that both Montenegro and North Macedonia have seen NATO membership as a fulfilling criterion for their integration into the European Union, although to date, it has not yielded the expected results.

2. Albania: From Warsaw to NATO

In the history of NATO's expansion in the Western Balkans, Albania is worth to be treated as a case study, not only because in the late 1960s it dared to leave its rival, the Warsaw Pact, but also for the fact that it was one of the first former communist countries, after the fall of its regime, to demonstrate a strong commitment to becoming part of NATO. During the Cold War, the geostrategic environment in the region formed a very interesting puzzle. Two of our neighbors, with whom we shared a maritime border, Italy and Greece, were members of NATO. The Italian coastline served as a deployment area for the U.S. Sixth Fleet. As for Greece, there were also several NATO bases with the primary purpose of securing the Mediterranean from the threat of the Soviet Union.

The solution to this "ex deux machine" puzzle would be the communist Albania, which would offer Moscow a golden opportunity to balance its power in the Mediterranean, given its geographical position. Albania's membership in the Warsaw Pact, in the political and military history of the Cold War, is now documented as a pragmatic move by the communist government to secure the territorial integrity of the country under the "umbrella" of a political and military collective security organization of the communist bloc led by the Soviet Union.[12] With the presence of Soviet military forces at the Pashaliman naval base and on the island of Sazan, rivalry with NATO would begin to take shape and would grow significantly.

NATO was treated as an "enemy" and a threat to the Albanian state, not only in political literature but also in military manuals and doctrines. However, knowledge of its military forces was a very important part of the military education of that period. It is worth noting that NATO's stance towards communist Albania was quite

[11] Senator Richard Lugar. NATO*: Out of Area or Out of Business. A Call for U.S. Leadership to Revive and Redefine the Alliance* (Washington, DC: Overseas Writers Club, 24 June 1993).

[12] Etleva Smaçi, *Albania in the Warsaw Pact*, UETPRESS, Tirana: 2023." Albania joined the Warsaw Pact in 1955, surprising the East more than the West. The reaction was related to several factors, starting with the extreme poverty of the communist country, as well as the change in Kremlin policy. The policy followed by Khrushchev after Stalin's death led to the expansion of the map of communist countries included in a military alliance in an extremely fragile region, such as the Balkans."

sensitive in the years 1955-1961, when the Soviet Union established a submarine base in the Bay of Vlora. As for NATO's stance following Albania's de facto exclusion from the Warsaw Pact, it was the adoption of the "hands off" policy, proposed by George Kennan in his February 1962 report.[13] The withdrawal of Soviet troops eased NATO's position in the Mediterranean, but the approach to Albania, a communist country, was calculated by NATO as a potential point of conflict with the Warsaw Pact.

This policy came to an end with the dissolution of the Warsaw Pact and the fall of communism. Emerging from a dictatorial isolation, Albania expressed interest in dialogue with NATO by becoming a member of the North Atlantic Cooperation Council (NACC) in June 1992. The journey toward NATO membership lasted nearly two decades.[14] It is worth noting that the membership process had characteristics similar to those of the Warsaw Pact in two aspects: politically partisan propaganda and popular enthusiasm about membership. The latter was often misinterpreted and treated more as a rapprochement with the U.S. rather than with a collective security organization.[15] This also explains the statistical data showing that about 90% of the population supported NATO membership (a stark contrast to other Balkan countries).

Partnership for Peace was a very important mechanism for preparing the former communist country, and member of the Warsaw Pact, for eventual membership in NATO[16]. Albania's accession to NATO came as a result of the significant decision to expand the Alliance, made on April 3, 2008, by the 26 heads of state and government of the Alliance during a special session of the NATO Summit in Bucharest, through which Albania and Croatia were invited to begin membership talks. Albania's first presentation as a full member of NATO took place at the NATO Summit held in Strasbourg/Kehl on April 4, 2009, while on April 7, 2009, the official flag-raising ceremony for Albania's accession to NATO was held at the Alliance's headquarters in Brussels.

Since the beginning of this journey, Albania's accession to NATO has been closely linked not only to reforms in the military sector but, first and foremost, to the democratization of life within the country, the fight against corruption, and organized crime. Unlike the traditional ideological approach of the communist regime, what needed to make Albania worthy of NATO membership was not only acceptance but also the adaptation to and embodiment of the common values symbolized by the

[13] National Archives Record Administration (NARA), Records of the U.S Department of State Relating to International Affairs of Albania, 1960-1963, Box 1926, November 17, 1961.

[14] Albania's inclusion in the alliance was supported by several instruments, such as the Partnership for Peace (PfP) and the Membership Action Plan (MAP), leading to its membership in 2009.

[15] Institute for Democracy and Mediation. Albanian perceptions on NATO integration. Tirana June 2007 http://idmalbania.org/publications/en/AlbPerceptionOnNATOintegrations.pdf.

[16] Albania responded positively to the invitation for the Partnership for Peace (PfP) in 1994. Later, as a result of positive steps, our country was included in the Membership Action Plan (MAP) in 1999

Alliance: a pluralistic system, democracy, freedom, and tolerance.[17] In contrast to other countries in the region, Albania did not face the same Russian factor in relation to its NATO membership; however, this does not mean that the accession was viewed positively by Moscow. Especially Albania's recent commitments to revitalize some military bases (such as the case of Kuçova), with a recent history tied to the Warsaw Pact, led the press to revisit the legacy of the Soviet camp.[18] Even before the opening of the Kuçova base, Russian platforms like Sputnik Serbia, along with other media operating in the Balkans, did not hesitate to spread fake news, portraying Albania as a "war corridor" to be used by NATO.[19]

Albania was depicted as a "puppet state" being exploited by the Alliance to militarize territories that, according to Sputnik, were already considered "occupied" by NATO. The revitalization of the Kuçova base has not only been a subject of interest for the press but has also been used by a category of pro-Russian scholars as an argument to claim that "the West has lied from the very beginning about its eastern expansion after the Cold War."[20]

The offering of Albanian territory for NATO bases appears unlikely to stop with the Kuçova base, as in statements made by Prime Minister Edi Rama in June of this year, it was mentioned that Albania is in discussions with NATO to build a naval base in Porto Romano[21], a port currently under construction on its Adriatic coastline. This announcement followed one made in May regarding Albania's offer to NATO of its Pashaliman naval base, located about 200 km (124 miles) south of Tirana, which is another Soviet-era legacy. The Pashaliman base is still the subject of ongoing debate with Moscow over the four submarines left there in 1961.

In conclusion, regarding the paradigm of Albania's transformation from "enemies to loyal friends" in relation to NATO, it seems that, after 15 years of membership, Albania is no longer merely a "consumer" of security, but also a provider of security, particularly for the Western Balkans region.

3. Expansion, Stability or Destability?

The early stages of NATO's expansion in the Western Balkans were marked by a noticeable hesitation. This reluctance became particularly evident at the onset of the war in the former Yugoslavia. NATO's own perceptions of some of the countries in

[17] NATO (2006b): Jaap de Hoop Scheffer, Secretary General, NATO, Speech at the Albanian parliament, 6 July, on-line text.

[18] In several instances, different platforms referred to the Kuçova base as 'a Soviet-era base.' Albania, wary of Russia, reopens Soviet-era air base to NATO | Reuters

[19] https://euronews.al/en/wars-of-the-west-propaganda-nato-will-attack-russia-through-albania-and-kosovo/ https://sputnikglobe.com/20240305/perennial-puppet-state-albania-logic The perpetual puppet state: Albania, a 'logical' choice for NATO's reorganization.

[20] Ibid.

[21] https://shqiptarja.com/lajm/Rama: Ready to Co-finance NATO's New Naval Base in Porto Romano; NATO Should Guarantee the Border Between Kosovo and Serbia"

the region were far from positive.[22] One of the most common questions raised in academic works is: Did NATO's expansion contribute to the democratic stabilization of post-communist states in the region? This question is also linked to the debate surrounding NATO expansion advocates like Warren Christopher, Anthony Lake, William Perry, Strobe Talbott, and others, who often used the argument of NATO's positive influence in consolidating democratic regimes in the post-communist period. It was anticipated that NATO's expansion in the Balkans would allow the Alliance to move away from its role as a "security importer" and instead enable it to "export" security to the region, ensuring stability through democracy and prosperity. Undoubtedly, for the Balkan countries that have joined NATO, this has translated into difficult political steps, though not impossible ones.

To overhaul their outdated institutions, all the Western Balkan countries aspiring to join NATO became part of new programs, with the most significant being the Partnership for Peace (PfP), established in 1994. The main goal of the PfP program was to strengthen cooperation and build reciprocal relations between partner countries.

Returning once again to the moment when the Alliance decided to expand and turn its attention to territories once considered a 'forbidden fruit,' in 1990, the Allies were very clear that 'in the new Europe being created, the security of every state was inextricably linked to the security of its neighbors.'[23] This same argument is reflected in Strobe Talbott's statement that "all of Europe will be safer and more prosperous if the former communist countries can move forward and develop through civil society, market economies, and harmonious relations with their neighbors."[24]

Talbott's argument is closely linked to his idea that NATO's presence in the former communist countries and, in some cases in former partners or satellites of the Soviet Union, was not merely a mechanism to contain Russia or a pressure tool, but a collective security instrument, which also included Russia itself. This explains why, after the end of the Cold War, the focus of the Alliance shifted from the defense of the territory of member states to the defense of shared interests, becoming a strategic necessity.[25] However, the above ideas belong to the last decade of the last century, when Russia was still reeling from the collapse of the Soviet Union and was considered "weak." After 2014, Russia's perspective on NATO's expansions shifted, treating new memberships as attempts by NATO to reshape the world order according to new borders.

---

[22] Watkins and Srdjan Gligorijević, NATO and the Balkans: A Case for Broader Integration, *Security Issues*, Institute for Mediation and Democracy, No. 5, Tirana: 2007.

[23] "*London Declaration on a Transformed NATO in the 21st century 26 Final March 19, 2001 North Atlantic Alliance,"* Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council. London July 5-6, 1990, paragraph 4.

[24] Strobe Talbott, "Russia Has Nothing to Fear," *New York Times*, February 18, 1997.

[25] Dr. William J. Perry and Warren Christopher. "NATO's True Mission." The New York Times, October 21, 1997

The first question that comes to mind is: Did NATO's expansion in the Balkans, a region where Russian influence has been constant in the international relations of the 20th and 21st centuries jeopardizes NATO-Russia relations?[26] Has NATO succeeded in creating stability in the region, as it argued for expansion, or was expansion merely a pretext, as Moscow claims?

Let us take a look at the countries that have joined NATO in the last decade, including Montenegro and North Macedonia. The latter is the newest member of the Alliance from the Western Balkans. In the case of North Macedonia, before joining the Alliance, NATO conducted three military operations to support peace, which not only contributed to resolving the internal conflict but also helped create the necessary conditions for consolidating democracy in the country. In the Balkan context, the case of North Macedonia is also seen as a success story regarding security issues in NATO-EU cooperation.[27]

What stands out in the case of North Macedonia is that its NATO membership did not have widespread popular support. Nationalist circles with Russian influence exerted pressure on certain segments of the population that opposed NATO's role. Russia attempted to capitalize on such difficulties to block North Macedonia's integration into NATO. The Kremlin condemned the name change as an imposition by the West and insisted that it be renegotiated in the UN Security Council, a forum in which it holds veto power. Nevertheless, Russia lacks the historical affinity with North Macedonia that it shares with Serbia. As a result, with North Macedonia's NATO membership, Russia has reduced its interest in the country. This shift has been evident in the softening of Kremlin statements on Macedonian issues and the redirection of aggression towards NATO, as it seeks to prevent further Balkan countries from joining the Alliance.

The same phenomenon was observed after Montenegro's accession in 2017, where the perspective shifted from a national to an international issue. The response to the cases of Montenegro and North Macedonia has been interpreted as Russia's return to the Balkans, where it seeks to regain the role it held as the Russian Empire until its collapse. From this perspective, Putin's Balkan strategy can be considered an important factor, driven by nationalist sentiments that he uses to appeal to his electorate, which, in turn, makes Russia's foreign policy more unpredictable than it was during the Soviet era, particularly during the Cold War.

Finally, as mentioned earlier, Serbia's non-involvement in NATO, despite being a significant player in the Balkans, makes it difficult to create stability and inevitably allows for Russian influence. Serbia stands as a "thorn" between an expanding NATO and Russia, its traditional partner. Can Serbia respond in a way that could be

[26] Dimitar Bechev, *Rival Power, Russia in Southeast Europe'.* Yale University Press. The author analyzes the thesis of pan-Orthodoxy and pan-Slavism.

[27] The signing of the Ohrid Agreement, to prevent the war in the former Yugoslav Republic of Macedonia.

harmful to the region? Russia, led by President Putin—a former Soviet official who moved from prime minister to president—has not been able to "swallow" NATO's "open door policy."

But for experts in Putin's foreign policy, this is less about a revival of the "Great Russia" concept and more about forcing the West to see Moscow as an equal player at the table.[28] In other words, Putin is attempting to recreate the Cold War-era bipolarity in the Balkans, after nearly a decade (1990–2000) of unipolarity established by NATO. The overall expansion (not just in the Balkans) has been seen by Moscow (particularly nationalist circles) as a "second Yalta," but without Russia. For many scholars, stability has been replaced by the term "stabilocracy," as NATO member countries have remained far from integration into the EU. However, both the Alliance and the countries of the region agree that the Western Balkans needs NATO to continue being politically committed to the region.[29]

Conclusions

The Western Balkans represents NATO's oldest and most enduring political and operational investment, and certainly the most challenging, given the regional complexity and its political, ethnic, and religious fragmentation. The region includes NATO member states, NATO partners, a neutral country (Serbia), and, finally, it is the region where NATO is still conducting its only military operation through KFOR in Kosovo.

It is undeniable that NATO's expansion as a whole, including its expansion into the Western Balkans, has sparked debate regarding Russia's intentions**.** Referring to Henry Kissinger, even in the early stages of NATO's expansion into Central and Eastern Europe, he expressed concern over Russia's "resentments," which he believed would manifest in efforts to "undermine" NATO in the newly acquired territories.

In the framework of Putin's foreign policy, this would translate into the theory of "zero-attacks," meaning that every Western victory is a pure loss for Moscow. NATO's expansion has been seen by Moscow as a manifestation of Washington's aspirations for hegemony in the Balkans. However, to conclude all the arguments presented, regional stability, in opposition to hegemony, is the strategic reasoning that best explains NATO's expansion in the region. In NATO's policy, we can certainly identify an effort to contribute to the democratic stabilization of the countries of the Western Balkans that have already joined the Alliance.

---

[28] Dimitar Bechev, "Understanding Russia's Influence in the Western Balkans," September 2018. The visit of Chancellor Angela Merkel and Secretary of Defense James Mattis to Skopje before the September 30 referendum was an indication that Russia was ready to undermine and manipulate the popular vote.

[29] Speech by NATO Secretary General Jens Stoltenberg previewing the NATO Summit in Brussels at the event organized by NATO, The German Council on Foreign Relations (DGAP) and The Brookings Institution

On one hand, as this study shows, the push for NATO's expansion in our region may not have had as significant an impact on democratization as its supporters hoped when they initiated the process in the mid-1990s. On the other hand, the expansion has had a very positive effect on Euro-Atlantic security. In other words, where NATO's "neighbors" are stable, NATO is "calm and secure." This means that the Alliance has sought to consolidate the vision outlined by Secretary of State Albright at the 1997 meeting, where she stated that the goal of further expansion steps was to "do for Eastern Europe what NATO had done 50 years earlier for Western Europe: integrate new democracies, eliminate old animosities, support economic recovery, and prevent conflicts."[30] The events in the Balkans in the early 1990s had a profound impact on NATO's evolution after the Cold War, and conversely, NATO's active presence in the region has not only prevented the outbreak of hostilities and nationalist fires but has also helped each of the Western Balkans states individually to successfully become part of the Euro-Atlantic zone.

Despite the reduced risk of serious armed conflict, the peace in the region remains fragile. Therefore, the Alliance must reassess its strategies towards the region to address current challenges. Prevention and defense will remain the cornerstones of NATO, and thanks to the practical implementation of NATO's open-door policy, most Western Balkan countries, now allies, contribute actively to it. Thus, it is widely accepted that no future vision of NATO can fail to include the entire Western Balkans, not just in the current framework of 3 inside, 3 outside.

Note: *All the ideas expressed in this article belong to the author and not to the institution where she works.*

Bibliography

1. Albright, Madeleine. Prepared Statement before the North Atlantic Council, NATO Headquarters, Brussels, Belgium, February 18, 1997
2. Bechev, Dimitar *"Understanding Russia's influence in the western Balkans"*, September, 2018
3. Bechev, Dimitar *Rival Power, Russia in Southeast Europe'.* Yale University Press.
4. Brzezinski, Z and Lake, A, *The Moral and Strategic Imperatives of NATO Enlargement.* International Herald Tribune, 1 July 1997.
5. Kissinger, Henry, *A World We Have Not Known*, Newsweek, 27 January 1997
6. Smaçi, Etleva. *Shqipëria në Traktatin e Varshavës (Albania in the Warsaw Treaty)*, UETPRESS, Tiranë:2023

[30] Madeleine K. Albright, Prepared Statement before the North Atlantic Council, NATO Headquarters, Brussels, Belgium, February 18, 1997.

7. Talbott, Strobe *The Russia Hand*, The Random House Trade Paperback Edition, 2003.

8. Zamfiresku, Elena. *NATO and Balkans*, Perceptions Journal of International Affairs, March-May 1999, Volume IV, Number 1.

9. Holbrooke, Richard *America, A European Power*, Foreign Affairs, March/April l995.

10. Perry, W and Warren Christopher. *NATO's True Mission*. The New York Times, October 21, 1997.

11. Watkins and Gligorijeviç, S. *NATO and the Balkans*: Example for broader integration, Security Issues, Institute for Mediation and Democracy, No. 5, Tirana: 2007.

Archival Sources

12. National Archives Record Administration (NARA), Records of the U.S Department of State Relating to International Affairs of Albania, 1960 -1963, Box 1926, November 17, 1961.

Internet Sources

13. Albania, wary of Russia, reopens Soviet-era air base to NATO | Reuters

14. https://euronews.al/en/wars-of-the-west-propaganda-nato-will-attack-russia-through-albania-and-kosovo/https://sputnikglobe.com/20240305/perennial-puppet-state-albania-logic

15. https://shqiptarja.com/lajm/Rama: Ready to Co-finance NATO's New Naval Base in Porto Romano; NATO Should Guarantee the Border Between Kosovo and Serbia"

16. http://idmalbania.org/publications/en/AlbPerceptionOnNATOintegrations.pdf

IV Modernization of the Greek army restores the dilemma of "guns vs butter" policy

Dr. Glevin DERVISHI
Head of Department at the Faculty of Security and Defense, AAF

Abstract

This article makes a survey of the national security challenges, foreign and domestic policy, as well as their reflection on the expenditures made by Greece in the field of defense. Greece has had a specific approach regarding national defense spending throughout the existence of the modern Greek state. Since its genesis, national defense, protection of sovereignty and territorial independence have been of vital importance to Greece, moreover beyond the normal functions of a state. This is one of the primary tasks for which a state exists, but in the case of Greece, the fulfillment of these tasks is at the limits of sacrifice [1].

This relationship has had its own deep historical reasons behind that have influenced in this trajectory. But the challenges presented by the Turkey-Cyprus-Aegean trinomial are precisely at its foundation, a trinomial with a direct impact on Greek foreign policy and national security issues. The strained historical relationship with Turkey, territorial claims on the islands, airspace management and the delimitation of the Continental Shelf along with the maintenance of the Aegean status quo have been a constant source of tension between the two NATO member states. Greece Defense expenditures are among the highest in the world in relation to the budget, exceeding the value of 4.6% for almost 45 consecutive years, followed by Cyprus with 3.8% of the budget. Greece ranks as the 26th country in the world and the first in Europe for military spending. While according to the Stockholm Institute for Peace Research SIPRI, Greece was ranked as the 5th country in the world to purchase conventional weapons for the years 2005-2009, with almost 6.14 billion dollars in purchases, but during the years 2000-2004 it held the 3rd place in the world for these purchases.

[1] Lynn, Mathew. *Bust - Greece, The Euro, And The Sovereign Debt Crisis*. London: Bloomberg Press, 2012.p. 114.

Under the constant pressure of a military power like Turkey, and often as a game victim of great powers, moreover of the war lobby to promote the arms race, Greece has had to make extraordinary and unaffordable expenses as regards its finances. It was precisely the military expenses that constituted the essence of the country's debts in the four times that Greek finances went bankrupt. The purchase of anti-aircraft missile systems, submarines, warships and military aircraft have been accompanied by a financial bill of nearly 110 billion euros, or 1/3 of the last debt of 330 billion euros that Greece borrowed [2].

Keywords: delimitation, military spending, national defense, trinomial Turkey-Cyprus-Aegean, territorial contradiction, status quo, Exclusive Economic Zone, Continental Shelf, naval power, etc.

1. Complex challenges of national security, a strategic trap to Greece

Turkey-Cyprus-Aegean trinomial constitutes Greece's existential base concerning foreign and domestic politics as well as national security. The maneuverability space in the long and short term is built on this trinomial, as well as the development, defense and policy-making space of Greece is designed. The nature of this trinomial, as sacred as difficult for Greece, constitutes the constant challenge that it must face, because the most difficult balances and the most unequal power distribution ratios possible are found in the system of this trinomial. In the view of Greece's foreign, domestic and security policy, the constituent elements of the trinomial, which are inseparable, interdependent and influencing each other, are seen as:

Turkey, together with sub-issues, is a priority issue of national security for Greece's foreign and domestic policy.

Cyprus, along with the islands of Crete, Corfu, and Sicily once constituted the corners of control in the Aegean during ancient Greece, and nowadays, whoever controls Cyprus projects power in the Middle East and Southern Anatolia.

The Aegean, together with its own elements, is existential, because trade, defense, transport and communication are connected with it. As regards Greeks, " There is no Greece without Aegean."

Greek-Turkish relations are characterized by difficult historical relations and territorial contradictions for specific areas of the Aegean Sea regarding the sovereignty of the sea and air space over the islands, as well as the expansion of the vital space over these areas.

The permanent conflict climate between the two countries lays on a deep historical ground with great divergences and inequalities. This relationship has several layers, starting with problems carried over from the past, territorial claims, the respective

[2] Manolopoulos, Jason. - *Greece's 'Odious' Debt. London*: ANTHEM PRESS, 2011.p. 71

minorities, the role of religion in this relationship as well as the use of third actors by both sides in view of possible diplomatic or military confrontation between Greece and Turkish. Difficult relations with Turkey have shaped the Greek tradition of the country's reliance on the Armed Forces as the biggest guarantee to ensure national security.

Cyprus, as the other element of the trinomial, has been the dilemma that has dominated Greece-Turkey and Turkey-EU relations in the last 50 years. The big difference in how the parties think of the political solution of the island issue, but also the military clash of 1974, have left an indelible mark on the Greek and Turkish political scene. For Greece, Cyprus is not only a matter of national historical importance, but Cyprus is vital for the entire region of the Eastern Mediterranean and the Middle East. Cyprus and Crete are equally important, as they serve as a static aircraft carrier in the Mediterranean Sea and can be used as a military base to control the Mediterranean and Anatolia[3]. The air space of Cyprus and Crete is an important intersection of air passages that connect Europe with Asia, the Middle East with the Caucasus, so such a position of Cyprus makes Turkey very interested in the island[4].

The importance of the island and its past has meant that British military bases are still located on the island today and are stationed in Olympus, where there is a radar base in Larnaca, Limassol and Akrotiri, in which 25,000 British troops are stationed. There are still about 40,000 UN troops on the island, as well as about 40,000 Turkish troops in Turkish Cyprus. The January 1996 crisis generated by the dispute over sovereignty over Imia/Kardak Island brought the level of confrontation between the two countries to the brink of armed conflict. But that crisis did not remain localized. Turkey repositioned its stance and resubmitted its claim that Kardak is Turkish and many other Aegean islands are under discussion.

To put Greece in positions of weakness, Turkish army units deployed in Northern Cyprus were settled along the Green Line and repositioned for the Battle of the Aegean. This tactical move put Greece in a delicate position, because from an uninhabited island all the bordering islands of the Aegean are now put into question and, above all, the status quo of Cyprus, moving into a new phase of the conflict and immediately the Chief of the Staff of the Greek-Cypriot army requested the establishment of a common defense doctrine with Greece. This proved once again that several issues are related to the Aegean: the demilitarization of maritime and air spaces, Cyprus and national security. As far as Greece is concerned, the preservation of sovereignty lies at the basis of relations with Turkey, and in this case, the Greek military caste proposed to the leadership not to retreat in the face of Turkish pressure, because if the precedent was created, many national balances would be called into question[5].

---

[3] Ahmet Davutogllu, *Thellësia Strategjike.* Shkup, 2010. Logos, p. 221.

[4] Turkish Ministry of Foreign Affairs, Relations with Bulgaria. Ankara, 2010.

[5] Michael Robert Hickok, *The Imia/Kardak Affair, 1995-96. A Case of Inadvertent Conflict*. European. Security, 19 June 2008 p.186.

The Aegean, together with its elements, is existential for Greece and Turkey, because trade, defense, transport and communication are connected to it. As regards Greeks, "There is no Greece without the Aegean". The Aegean is the most typical case of a maritime region which connects not only issues of maritime law, but also those of history, security, trade, maritime and airspace. On the Aegean, the space of maneuverability is built in the long and short term, as well as the space of development, defense and policy-making of Greece and Turkey is projected.

The Aegean in itself is connected with a complexity of issues, such as: the delimitation of the Territorial Sea (determination of maritime borders with coordinates), the delimitation of the Continental Shelf, the Exclusive Economic Zone, the airspace, the management of civil and military air traffic and the militarization of the islands. Greece finds support in international law and in the bilateral framework, such as: the Treaty of February 10, 1947[6] for peace with Italy, which gave Greece the 12 islands of the Dodecanese and some island rocks, leaving open a territorial fire between the two countries, do not clearly define the list of island rocks that pass Greece[7]. The Aegean is often considered as the most fragile point of bilateral relations and as the battlefield in which strength is demonstrated, pulse is taxed and strategy is built on the opponent. The Aegean islands are divided into 6 main groups: North Aegean, North Sporades, Cyclades, East Aegean, Dodecanese and South Aegean. These islands occupy an area of almost 23,000 km^2, which is about 10% of the total area of the Aegean Sea[8]. In 1931, Greece declared the width of its territorial waters to be 10 miles, but this move was not well received by the Great Powers, who asked Greece to reduce the width of its territorial waters to 6 miles, and in 1936, Greece decided to keep the 6-mile limit, which is still in force in the Aegean. Greece's strategic objective is to progress through the expansion of the Territorial Sea from the current 6 miles to 12 miles, because this expansion would add to Greece its maritime and air space, the Exclusive Economic Zone and the Continental Shelf, which enables the use of underwater assets and natural resources. Currently, the Aegean is divided according to these ratios: 7.5% of it belongs to Turkey, whereas Greece owns 43.5% and 49% is international sea. The full implementation of the Montego Bay Convention gives Greece the possibility of using from the current 43.5% to 71.5% of the sea and air space of the entire Aegean; 8.7% for Turkey

[6] Në seksionin V - Greqia, të Traktatit të Paqes mes Italisë dhe Greqisë në nenin 14 thuhet:
1. Italia me anë të këtij traktati i jep Greqisë sovranitet të plotë në ishujt e Dodekanezit të përmendur më poshtë, Stampalia (Astropalia), Rhodes (Rhodes), Calki (Kharki), Scarpanto, Casos (Casso), Piscopis (Tilos), Misiros (Nisyros), Calimnos (Kalymnos), Leros, Patmos, Lipsos (Lipso), Simi (Symi), Cos (Kos) dhe Castellorizo, si dhe ishujt e tjerë të vegjël ngjitur.
2. Këta ishuj do të jenë dhe do të mbeten të demilitarizuara.
3. Procedura dhe kushtet teknike që rregullojnë transferimin e këtyre ishujve te Greqia do të përcaktohen me marrëveshje midis Qeverive të Mbretërisë së Bashkuar dhe Greqisë dhe do të merren masa për tërheqjen e trupave të huaja jo më vonë se 90 ditë nga hyrja në fuqi e këtij traktati.

[7] Ahmet Davutogllu*, Thellësia Strategjike.* Shkup, 2010. Logos, p. 196.

[8] Ibid., p. 215.

and 19.2% will remain international sea[9]. This is an unacceptable fact under any circumstances referring to Turkey, which claims that, by applying the width of 12 miles provided by this convention, the Aegean will turn into a Greek internal sea [10].

According to Ankara, the full implementation of this criterion of the convention would bring losses for Turkey, while the international waters between the two states would decrease drastically. Consequently, access to the ports of Istanbul and Izmir would be limited to the maximum and therefore, this contradicts the Turkish maritime doctrine of "Blue Country"[11], which aims to expand Turkey's maritime spaces and its ambition as a naval power. In order to legitimize the situation and increase the possibility of its actions, Greece ratified in the parliament the new law of the sea no. 2321, on June 1, 1995, by recognizing its right to expand the Territorial Sea from 6 to 12 miles at a convenient time. On June 7 of the same year, the Turkish parliament ratified a resolution. It charged the government with protecting the territorial independence, maritime and airspace of Turkey in the Aegean by any means, in case it sees that Turkish sovereignty is being violated. The direct result of this decision of the Turkish parliament is the political attitude of the Greek Presidency, for the reason that, since 1995 no Greek president has made official visits to Turkey, thus expressing their protest against Athens. In 1995, Turkey accused Greece that it was preparing the population of the uninhabited islands of the Aegean, which do not have a clear legal and political status. Moreover, this contradicts the Peace Treaty between Italy and Greece, which provides their demilitarization[12] accordingly.

These islands and the areas around them are considered as gray areas and without legal status according to Ankara; whereas Greece considers them as part of its sovereignty. But it is clear that Athens, unilaterally, through the use of force cannot resolve the issue of sovereignty over the Aegean, and even more it is clear that Ankara cannot tolerate at any time to recognize the full sovereignty of Aegean to Greece.

The Treaty of Lausanne decided that the territorial sea of the lateral states was up to 3 miles in 1923. Greece extended its territorial waters to six miles in 1936, and the current status quo was formed when Turkey accepted the 6-mile limit in 1964. According to the UN Convention on the Law of the Sea (UNCLOS) which was signed in 1982 and came into effect in Greece in 1995, signatory states have the right to extend their territorial waters up to 12 miles. Greece, unlike Turkey, has signed UNCLOS Convention in 1982, and it considers determining the width of territorial waters as a sovereign right and also claims that it will expand its territorial waters at

[9] Tozun Bahcheli*, "The potential for conflicts in Greek -Turkish Relations",* London, The Guardian, 1999, p. 26.

[10] Ahmet Davutogllu, *Thellësia Strategjike.* Shkup, 2010. Logos, p. 216.

[11] *https://www.ifri.org/en/publications/etudes-de-lifri/mavi-vatan-blue-homeland-origins-influences-and-limits-ambitious* Mavi Vatan, the "Blue Homeland"*: the Origins, Influences and Limits of an Ambitious Doctrine for Turkey,* Aurélien DENIZEAU, Etudes de l'Ifri, April 2021.

[12] Treaty of Peace with Italy: *https://www.loc.gov/law/help/us-treaties/bevans/m-ust000004-0311.pdf*

a convenient moment. Turkey has not signed the Convention and Ankara considers this threatening Greek action as a casus belli. Greece claims that the Turkish positioning as a casus belli is against Article 2, paragraph 4 of the UN Charter, according to which members cannot threaten the territorial integrity of the others. Turkey assumes that its position stems from Article 300 of UNCLOS, according to which parties can exercise rights recognized by UNCLOS, but without abusing with these rights. According to Turkey, the Aegean is a semi-enclosed sea that requires the application of specific rules. On the other hand, Greece does not consider the Aegean as a semi-enclosed sea, so that it makes the 12-mile limit applicable consequently[13]. The current status quo seems to be the best solution for both countries, although it does not guarantee stability in bilateral relations [14].

Flight Information Region (FIR - Athens/Flight Information Region), is another hot spot between the two countries connected to the Aegean, defined in 1950, based on the ICAO convention of 1944, which charges states with maintaining and managing their airspace. Ankara, in addition to Greek claims for maritime space, has also rejected claims for airspace over the Aegean. Regarding to Turkish leaders, Greece abuses the right to hold responsibility for the Flight Information Region (FIR) in the Aegean. According to Turkey, Greece violates the 1944 Chicago Convention on FIR when it requests flight plans for flights of Turkish military and civilian aircraft in international space over the Aegean. Furthermore, Turkey has refused to accept the Greek claim of 10 miles as the limits of its airspace in the Aegean, as it does not correspond to the 6 miles that Greece enjoys as maritime borders in this area. In 1950, Turkey accepted (FIR - Athens) which includes Greek airspace and some areas of international airspace, but FIR - Athens is violated on average 10 times per day and the Greek national airspace is violated on average 4 times per day by Turkish warplanes.

2. To balance the Turkish ambition, between the foreign policy and the increase of defense capacities

Greek-Turkish relations remain at the top of the Greek foreign policy agenda. During the last forty years there have been three major crises in Cyprus, three more in the Aegean, as well as a number of "hot" incidents. Relations between Greece and Turkey, two NATO allies in the Eastern Mediterranean, remained strained after the end of the Cold War, while the traditional cycle of "conflict-negotiation-conflict" prevails as a common feature of the new era. In order to enable a secure and constant environment, Greece is interested in Turkey to remain anchored in the club of Western countries; furthermore, to remain politically and economically engaged with the West to enable its modernization, because a Turkey with an aggressive

[13] Yaprak Gürsoy, *Regime Change in the Aegean after the Second World War: Reconsidering Foreign Influence.* Journal of Modern Greek Studies, Volume 27, No. 2, October 2009, (Article) Published by The Johns Hopkins University Press, p. 347.

[14] *Ahmet Davutogllu, Thellësia Strategjike. Shkup, 2010. "Logos", p. 217.*

behavior and far modernization, is a constant concern for Greece. Regardless of the quiet and normal periods that this bilateral relationship may have, this relationship will be at the center of the Greek focus, and why Greece can gain self-confidence through its active play in bodies such as the EU and NATO. The regional and international security environment will remain variable and unstable, where, due to geography and economic prosperity, Greece will be strongly influenced by these trends. Demographic, political and socio-economic security, developments in the Mediterranean and the Middle East will increasingly strain the countries in the south of the EU, as regards threats coming from the Mediterranean. During the 21st century, relations with Turkey will dominate Greece's foreign and security policy[15].

Turkey's policy towards Greece has been perceived by Greek policymakers as influenced by Turkey's ambitions for regional hegemony and by its resentment of former colonial powers over their perception of Greece as a "difficult" and often "stubborn" country. but a small neighboring country and former part of the Ottoman Empire. Greek security planners are concerned about Turkey's revisionist intentions towards Greece, as it is expressed in official statements, diplomatic initiatives and military actions (including the deployment of its armed forces).

To balance threats to its security, Greece has relied on a combination of "internal" (strong armed forces) and "external balancing" (with participation in all political and security organizations of Western Europe, such as NATO and EU), as well as signing and acceding to practically all multilateral agreements on the control and international control regime of arms exports [16]. Small states have fewer opportunities and less freedom of maneuver than major powers to promote their security interests. But to do this as efficiently as possible, Greece has tried to raise its voice and integrate its policies with those of partners in the European Union and its allies in NATO, as mechanisms that generate a security environment. Greece has often used these organizations to control or supervise the Turkish military potential, using the strength of multinational mechanisms and their mediating and influencing role in controlling arms exports.

As reliance on the Western alliance proved to be rather ineffective, after the Turkish occupation of Cyprus Greece began to place more emphasis on "internal balancing" (by strengthening its own Armed Forces) and less on NATO membership and bilateral relations with the United States (mainly as a result of the US's "privileged" relations with Turkey). However, although efforts to internally balance the Turkish threat were generally successful, Greece managed to achieve its short-term goal of achieving a balance of power with Turkey, but the medium/long-term goal for Greece was and continues to be "salvation" from the endless arms race, so that this race does not deviate from its strategic goal: economic development and full integration into

[15] Ibid., p.6.

[16] Thanos Dokos, *Greek Defense Spending in Times of Crisis: The urgent need for defense reform*, Eliamep. March 2013, p. 2.

the European Union[17]. Greece has tried to move away from perceptions of zero-sum games compared to Turkey, and in general, both countries are much better off today in terms of bilateral relations (including trade and people-to-people contacts) than they were before 1999. Having said that, neither country has really budged from their rigid positions on "big policy" issues, as Greece and Turkey continue to perceive each other through a Hobbesian prism, where skepticism and mistrust continue to prevail. Among the "success stories" in Greek-Turkish relations, we can refer to the dynamics of "citizen diplomacy", through the increase of bilateral trade and energy cooperation (through the construction of the Turkey-Greece Interconnector (ITG), which transports natural gas Azer" in Greece through Turkey, with Italy as the final destination.

Most Greek policymakers continue to believe that it is in everyone's best interest for Turkey to remain anchored in Western institutions. But that may not be an option as far as EU members are concerned, as there is strong opposition in major European countries and also a growing sense of disillusionment in Turkey. Greece remains a supporter of EU membership for Turkey (provided that, of course, it is to meet the required criteria, have a solution to the Cyprus problem and return to full normal state Greek-Turkish relations); meanwhile, its influence within the EU in relation to Cyprus (where, apparently, there is no will on the part of Turkey and consequently little enthusiasm on the part of the Greek Cypriots for any meaningful mutual compromise) is quite limited[18]. Managing the often-difficult relationship with Turkey remains a high foreign policy priority for any Greek government.

Greece must avoid a new arms race with Turkey, and various ideas for reducing arms and strengthening confidence-building measures are repeatedly circulating. As long as the other side has generally not shown willingness, according to Athens, for such initiatives and there are still statements from Turkey about *casus belli*, so in order to have deterrent capabilities that will enable peace and stability in the Aegean, then Greece would have no choice but to have high defense expenses compared to other EU member states and to invest in technological superiority and the full use of its human resources, as well as strengthening strategic alliances.

Finally, Greece remains a full member of the EU and NATO, and both institutions are involved in various efforts for conflict prevention and stability in an increasingly unstable Europe. While Greece's strategic choice is to become deeply integrated into the European Security Architecture, Greece's security interests are also to serve through a preventive policy for conflicts, through early control of sources of instability, contributing to such efforts based on its capabilities. Therefore, Greece needs to structure a part of the Armed Forces in such a way as to increase interoperability and participation in EU and NATO multinational operations. However, current fiscal constraints and national defense priorities have relegated this from a priority

[17] Ibid., p. 3.

[18] Theodoros Pangallos, *Me Papandreun në Europë*. Tirana, 2017. "Toena", Publishing House p. 185.

objective to a secondary one. Indeed, Greece has significantly reduced its contribution to multinational missions (NATO and EU) in recent months, due to financial constraints. The long-term objective for Greece will continue to be to reconcile its international responsibilities with national interests and security, where major differences often arise.[19].

3. Modernization of the Armed Forces, as an instrument of prevention and to maintain the *status quo* with Turkey

Despite being a member of the EU and NATO, Greece is geographically located in a conflict region, where the use of force in interstate relations can still be considered an option (admittedly, in very specific circumstances). In fact, compared to other EU and NATO member states, Greek security concerns represent a unique case, which is reflected in both the level of human and material resources that the country allocates annually to its defense.

Given the above challenges, but mainly since 1974, the military forces of both countries have been placed on full alert in 1987, 1994, 1996 and 2022, where it has been difficult to avoid military conflict between Greece and Turkey. Facing these challenges has imposed on Greece the need for continuous military, political-tactical engagement and the continuous increase of defense capacities in the Aegean despite the costs and opportunities. To respond to the challenges, Greece opened the chapter of unbridled spending to maintain the *status quo* in the Aegean and to increase its reactive capacities against an aggressive and clearly dominant Turkey. Involvement in this vortex, where the side that does not keep up the pressure will accept the conditions, will quickly turn Greece into a client country and subject of the war lobby in the USA, England, Germany and France.

Sovereignty over the Aegean has led to a frightening arms race between the two countries and has made this area highly militarized. Billion-dollar in investments in military technology and the construction of naval and air infrastructure have significantly increased the impact on the Greek state budget. The situation in the Aegean is also influenced by a number of geostrategic factors, as Turkey, which lies in the vital space between Greece and Russia, checks the pulse of the region and these two countries through the strategic position of the two straits, which in the great geopolitical game shifts the tension to another level. Greece does the same with Turkey through the Aegean islands, limiting its vital space and maritime strategy[20].

The country's national security challenges from the northeastern and eastern borders have oriented the organization and distribution of the Armed Forces to the extent of 80% of its personnel and equipment in order to face threats, where efforts to protect the sea and air borders in the Aegean prevail. The positioning of military units is

[19] Thanos Dokos, *Greek Defense Spending in Times of Crisis: The urgent need for defense reform*. Eliamep, 2013, f. 11.
[20] Ibid., f. 196.

denser on the Aegean islands, starting with Lemnos, Lesbos, Chios, Samos, Kos, Rhodes and Crete, which constitute the perimeter of the defense of the ring of fire of the Greek-Turkish border. As a result of the constant challenges in national security and the need to maintain control, as well as to follow the technological pace to respond to the military capacities of its neighbors, Greece has had to make frequent investments in the field of defense, especially during the last 3 decades.

From 1996 to 2005, the Greek Army underwent a massive modernization and reorganization process, which focused on the modernization of the motorized units of mainland Greece, to adapt to new needs and to keep up with technological advances. This process aimed to reduce costs in order to have a more efficient army and, as a result, only a few field units were closed, failing to achieve the objectives set by the process[21]. Failure to achieve the objectives of the first plan led to the construction of a new modernization process based on a three-phase procurement program, started in 2006 and considered a realistic plan:

First phase: 2006-2010.

Second phase: 2010-2015.

Third phase: 2015-2020.

For the implementation of this plan, the financial bill was 22 billion euros, although the defense budget could only generate 37% of these needs, because cuts during the crisis years brought the defense budget below 3%, for the first time since 1974. Among the priorities of this plan were: the purchase of transport helicopters, infantry combat systems, maintenance parts and C4I. (*Command Control Communication Computers Intelligence*)[22]. This period of the extension of this three-phase plan was strongly influenced by the Greek economic crisis and as a result of the austerity measures imposed by the Troika, Athens was forced to reduce defense spending from 3.1% to 2.1% of GDP. According to the International Institute for Strategic Studies (IISS), Greece spends between 60-73% of this budget on military personnel, but the data presented best serves to analyze Greece's national defense strategy and the dilemma between "guns vs. butter policy".

The modernization and strengthening of all three branches of the Armed Forces is vital and necessary (due to the need for joint operations), where their role will be mutually supportive and reinforcing. By the very nature of the challenges but also geography, with a weak fleet, Greece would lose control of the Aegean (Middle East) and with a weak army it would not be able to defend its islands. Although the Air Force can by no means win a conflict alone, it can act as a strong deterrent in peacetime and if conflict avoidance fails, it can create a protective umbrella under which the other two forces can fight and win a war. Therefore, preventing enemy air superiority should be a top priority.

[21] Thanos Dokos, *Greek security policy in the 21-st century*. Eliamep, 2007, f.7.

[22] Ibid., f. 8.

Every year, Greece allocates a significant part of its income for national defense. Defense expenditures as a percentage of GDP are significantly higher than the EU average. Over the past decade, the Greek defense burden has been approximately doubled the average of the 27 EU member states. This is not a recent phenomenon, but rather a consistent pattern over the past five decades, due to the acute external security problems that Greece faces compared to its EU partners.[23]. Compared to its EU partners, Greece is in a category of its own when it comes to the national security challenges posed by its neighboring countries. Therefore, the need to invest scarce and valuable resources in national defense, while facing fiscal and economic difficulties, constitutes a burden to society. Thus, Greece is once again facing the difficult dilemma of "guns vs. butter policy". Greece is seeking to achieve both: preventing the conflict with Turkey, which is costing it dearly, and the need for economic development, constituting a major challenge for Greek policymakers.

After overcoming the difficult situation and the measures imposed by the Troika, Greece has returned to the tradition of increasing the country's military spending in order to deter Turkey. To make up for lost time, the Greek government presented an ambitious plan in early April 2024 to increase the country's military capabilities, thus marking "one of the largest reforms in the history of the modern Greek state," as Minister of National Defense Nikos Dendias stated. The aim of this ambitious modernization program, which foresees about 15 specific modernization priorities, is clear: to prepare the Greek Army for the challenges of the 21st century, by proposing some radical changes in weapons system, innovation, structure, personnel treatment, as well as by increasing national production capacities in the field of defense in order to preserve the sovereignty and national integrity of Greece. The program aims to affect the inventory of equipment for the three services, air, naval and land vehicles of the Greek Army.

In the Air Force, its modernization is aimed at achieving homogeneity in the current variety of vehicles as well as better interoperability of weapon systems and their maintenance parts, by removing from the inventory a large range of American and French models whose age and variety have greatly increased the country's financial bill. The objective to modernize part of the current fleet and to switch to the new 4.5 - 5 generation of jet aircraft by 2030, with a fleet of about 200 aircraft and the purchase of at least 35 American Black Hawk helicopters of the latest M version, seemingly too ambitious, has highlighted quite a few problems for the country.

In the Navy, Greece aims to become part of the joint production program of the "Constellation" class frigate to enable the construction of 7 frigates of this class for the Greek Navy in Greek shipyards. Meanwhile, during the last 2 years, Greece has signed a $ 5.9 billion agreement with the French company FNG for the purchase of 3 + 1 Belharra class frigates, within 2027 where work has already begun on their

[23] Thanos Dokos, *Greek Defense Spending in Times of Crisis: The urgent need for defense reform*, Eliamep. March 2013, f. 4.

production, which marks a historic moment for the Greek Navy after 30 years since the purchase of the Hydra class frigates of the Meko model from Germany.

In the Land Force, Greece aims to modernize its 500 existing Leopard 1A5 tanks, it will be equipped with 756 M-1117 armored personnel carriers during 2024, and will be equipped with a medium-altitude long-range unmanned aerial vehicle. The Greek government, in order to increase domestic military production, will pass through Parliament the establishment of the National Center for the Defense Ecosystem, which will be accompanied by several other legal initiatives that will enable the production of a series of unmanned aerial vehicles, anti-aircraft vehicles and anti-drone warfare vehicles.[24].

Exploiting the importance of the Aegean and engaging Mediterranean naval powers in the region (especially France) has been the focus of Greek diplomacy to secure a unique political-military partnership with France. On September 27, 2021, Greece and France signed a mutual defense pact, where Article 2 explicitly states that the parties come to mutual military assistance in the event of an attack by a third party. This pact, in addition to being accompanied by a package of defense asset sales by France to Greece, also constitutes an unusual precedent for two NATO member countries, where two members sign a mutual defense pact against another NATO member (potentially Turkey).

As can be seen from the plan, most of the focus and resources are on the Greek Air Force, as one of the key assets that even enjoys special attention in the military hierarchy, as the force under the direct supervision of the Chief of the General Staff of the Greek National Defense. Aviation is a very expensive and technologically variable weapon, which makes maintaining air superiority extremely difficult. The Greek aviation, due to the financial crisis that the country went through, has been facing for a long time the impossibility of purchasing 4.5-5 generation military aircraft. This force has about 230 aircraft and has a concentration of its strength mainly on the eastern borders of the country and in the Aegean, where tensions are often the basis for the excellence of the operational skills of the Greek air force, which is ranked among the most capable air forces in NATO.

The purchase of 24 Rafale twin-engine multi-role aircraft from France is undoubtedly one of the largest purchases under this plan and the most expensive for Greece in recent years. Greece and France have a long history of cooperation in the field of defense and mainly for the Hellenic Air Force, where in 1974 it bought Mirage F 1 aircraft, then in 1989 Greece bought 40 Mirage 2000 multi-role aircraft. The new Rafale 4.5 generation multi-role aircraft seem like an acquisition that will hardly justify the hefty bill of almost 3 billion euros, as the nature of this aircraft is extremely costly in operation, maintenance, combat systems, armament, technological supremacy and its range of almost 3700 km is beyond Greece's needs, moreover, their range is twice

[24] https://www.ekathimerini.com/news/1235320/dendias-unveils-ambitious-air-force-plans/

that of the Mirage 2000 aircraft or four times that of the 80 F-16 aircraft already undergoing modernization that are in the inventory of the Greek Air Force. These qualities go beyond the country's airspace, needs, nature of operations, capacities and range of action of this force, whose main mission is the protection of national airspace and not operating at great distances or beyond enemy lines.

If we analyze the fact that Greek fighter jets engage in an average of ten "scramble" missions over the Aegean, which often end in "dog-fights", taking off every day with aircraft such as the Rafale is beyond any economic logic and from a tactical point of view debatable, since they are a model that justifies the costs of deep interception and strategic bombing. The largest operating distances are in the airspace of Albania and North Macedonia within the framework of air policing as NATO countries. This purchase clearly has a strategic political nature, to have France on its side, as evidenced by the tension in the Aegean during the missions of the Turkish naval group led by the ship Oruc Reis. France's role in the EU as well as the presence of the French military fleet during the summer of 2022 in the Aegean and the Eastern Mediterranean gave Greece psychological security but on the other hand helped as a deterrent force for Turkish actions. It seems that the Rafale aircraft squadrons will now also have a deterrent role, but for a small country like Greece, with limited finances, it is a great luxury to keep such an asset mainly for this function. In other words, it is a purchase of the Greek Ministry of Foreign Affairs and not of the Ministry of National Defense, as a purchase imposed by the geopolitical circumstances in the Aegean and not by military needs. This purchase has reconfirmed once again the consolidated role of the Ministry of Foreign Affairs in the national security of Greece, often decisive even in front of the Ministry of National Defense.

Conclusions

In the Greek defense doctrine vis-à-vis Turkey, the solution to the strategic dilemma that Greece faces will be based on the "Flexible Response", which is based on the creation of special solutions in cases of crisis management, but taking care to avoid military clashes and, at the same time, not allowing a situation where Greece withdraws from its mission to protect the islands and the rights over them. To enable the implementation of a flexible response, Greece will need to expand its military capabilities in a continuous but rational manner, which would guarantee the preservation of its space and strategic interests in the Aegean, but this risks once again putting national finances in the trap of cyclical crisis. Faced with national security challenges, Greece seems to be choosing to deepen military expenditure with a very sublime motive and well understood by its citizens: that of the national defense expenditure.

In the context of an intense endeavor by Turkey to project itself as a medium-great power and with programs to increase military capabilities to levels of absolute autonomy on the part of Turkey, Greece is quickly placing itself in the position that it will have to make up for lost time during the years of crisis. A Turkey in search

of status as a military power in the region and beyond is predisposed to be more inclined to implement an active military policy. Towards a modern naval force, a modern combat aviation, increasing defense capabilities and keeping life alive on the Aegean islands by providing services and opportunities for the islanders, will be a challenge that Athens will continue to face.

On the other hand, the initiated processes of confidence-building mechanisms, diplomatic consultations and exploratory consultations will always continue to be a mechanism for reducing pressure and managing situations beyond normal operation between the two countries, but without achieving concrete results, since every decision for advancement or for finding a final solution between the two countries, in addition to engaging the diplomatic apparatus of both countries, is ultimately a product that combines diplomacy, defense, leadership, finance, regional balance reports, the involvement of international actors and the time factor. The progress of bilateral relations in the region where the two countries are located and the interconnection of a number of interests of great powers will continue to keep all major global actors engaged in the progress of this relationship.

References:

1. Akiman, Nazmi. *Turkish-Greek Relations: From Uneasy Coexistence to Better Relations*, in: Mediterranean Quarterly: Summer 2002.
2. Bahcheli, Tozun. *The potential for conflicts in Greek -Turkish Relations*. London: The Guardian, 1999.
3. Davutogllu, Ahmet. *Thellësia strategjike*. Shkup: "Logos", 2010.
4. Dokos, Thanos. *Greek Defense Spending in Times of Crisis: The urgent need for defense reform*. Eliamep, March 2013.
5. Gürsoy, Yaprak. *Regime Change in the Aegean after the Second World War: Reconsidering Foreign Influence*. Journal of Modern Greek Studies, Volume 27, Number 2, Published by The Johns Hopkins University Press, October 2009.
6. Hickok, Michael Robert, *The Imia/Kardak Affair, 1995-96. A Case of Inadvertent Conflict*. European Security, 19 June 2008.
7. Kassimeris, Christos. *Greek response to the Cyprus invasion*. European University, Cyprus: Small Wars & Insurgencies. Vol. 19, No. 2, June 2008. 57.
8. Kassimeris, Christos. *The Inconsistency of United States Foreign Policy in the Aftermath of the Cyprus Invasion: The Turkish Arms Embargo and its Termination*. Journal of Modern Greek Studies, Volume 26, Number 1, May 2008.
9. Pangallos, Thedhoros. *Me Papandreun në Europë*. Tiranë: "Toena", 2017.
10. Lynn, Mathew. *Bust - Greece, The Euro, And The Sovereign Debt Crisis*. London: Bloomberg Press, 2012.
11. Manolopoulos, Jason. *Greece's 'Odious' Debt*. London: ANTHEM PRESS, 2011.