AD SECURITATEM

THE BEST ESSAYS BY COURSE PARTICIPANTS
AT THE BALTIC DEFENCE COLLEGE

ACADEMIC YEAR 2024/2025

BALTIC DEFENCE COLLEGE

Contents

BEST ESSAYS OF THE JOINT COMMAND AND GENERAL STAFF COURSE

MAJ Diego Callirgos. Empowered by Drones: Civilian Resistance in the Russo-Ukrainian War

Introduction

On the 24th of February 2022, reports of explosions throughout Kyiv and the eastern regions of Ukraine heralded a major escalation in the Russo-Ukrainian War. The Russian Federation proceeded to launch a series of offensives into Kyiv and postured a 64-kilometre-long convoy of mechanized vehicles and supply trucks to the north of Ukraine's capital. However, this massive convoy was remarkably derailed to a halt in advance of Kyiv. A Ukrainian commander recounted that this was 'in significant part because of a series of night ambushes carried out by a team of 30 Ukrainian special forces and drone operators on quad bikes' (Borger, 2022). Later reports identified these drone operators as members of the non-governmental organization, Aerorozvidka. This group of Ukrainian civilians, empowered by drones, helped counter an overwhelming force that threatened the capital of their nation.

Resistance, according to Joint Special Operation University's (JSOU) *Resistance Operating Concept* (Fiala, 2020), is

> 'A nation's organized, whole-of-society effort, encompassing the full range of activities from nonviolent to violent, led by a legally established government […] to reestablish independence and autonomy within its sovereign territory that has been wholly or partially occupied by a foreign power.'

Aerorozvidka's defence of Kyiv exemplified one way that drones can empower Ukraine's resistance. Yet, separate reports highlight many other ways that civilian activists are leveraging drones to contribute to the war effort. For example, we see Ukraine's citizens organizing drone donation drives for defense forces. We see tech-savvy students and hobbyists engineering their own drones to gift to their frontline soldiers (O'Grady, Khudov, 2024). We also see examples of first-person view drone-recorded war videography enabling Ukraine's civilians to engage in information operations on social media (Panella, 2023). By all accounts, we see how the relationship between drones and civilian activists can contribute to homeland defence. Drones are ubiquitous to modern warfare but in Ukraine we can uniquely examine how they supplement the efforts of a state populace resisting occupation. This research seeks to aggregate and analyse publicly available sources that demonstrate how Ukrainian civilians are interfacing with drones in support of resistance objectives. It will ultimately seek to address the research question: **How do drones uniquely empower Ukraine's civilians to contribute to national resistance against Russian occupation?**

This paper will argue that **Ukraine's resistance to Russian occupation demonstrates that drones can uniquely empower civilians by providing accessible, versatile, and scalable means to contribute to total defence.**

To support this thesis, we will address the specific circumstances in Ukraine that make drones a highly *accessible* platform for civilian resistance activities. First, we will contextualize conditions specific to Ukraine’s total defence that enable the role of drones in civilian resistance. With this foundation, we will continue to expand on accessibility throughout this paper as we examine how drones are specifically applied to civilian resistance objectives.

To validate the *versatile* civilian applications for drones, this paper will use the Proximate Resistance Objective (PRO) framework developed by Rand researchers, for the Baltic States (Binnendjik, Kepe, 2021) which was later adapted to analyse Ukraine’s resistance (Kepe, Demus, 2023). This framework aligns with the Resistance Operating Concept and defines the five PROs below that correlate with successful outcomes in civilian resistance (Binnendjik, Kepe, 2021):

- **PRO-1**: Imposing Direct or Indirect Costs on an Occupying Force
- **PRO-2**: Securing External Support
- **PRO-3**: Denying an Occupier’s Political and Economic Consolidation
- **PRO-4**: Reducing an Occupier’s Capacity for Repression
- **PRO-5**: Maintaining and Expanding Popular Support

As we explore specific means that Ukrainian civilians apply drones to resistance, we will orient those diverse actions towards relevant PROs. Concurrently, we will address *scalability* through a three-tier construct. First, we will determine concrete ways *individual* Ukrainian civilians can deliver specific effects in support of resistance. Then we will examine how drones help marshal *community* efforts in support of the war effort. Finally, we will scale these civilian efforts to the *national* level to examine the aggregate effects that drones provide towards Ukraine's total defence. By coalescing these echelons, we can observe how contributions to PROs are magnified when civilians collectively scale their efforts with drones as a common platform.

1. Background: Civilians, Drones, and Ukraine's Total Defence

For the past two decades, drones have trended towards ubiquity in the tactical battlespace as seen in the Syrian Civil War, the Second Libyan Civil War, and Nagorno-Karabakh conflict. Academic consensus harkens that drones are a defining feature of the Russo-Ukrainian War with at least one scholar claiming it holds the title of the first 'drone war' (DeVore, 2023). To examine how drone's ubiquity in war empowers Ukraine's civilian resistance, we must first contextualize how the Ukraine's government enabled their use in support of total defence.

Total Defence, according to the JSOU framework, aggregates all activities applied to defend a nation's independence, sovereignty, and territory. It marshals civil and military efforts from the local to national level including individuals, volunteer groups, commercial enterprises, and government agencies (Fiala, 2020). The conditions we will examine that translate this doctrine to drone-enabled civilian resistance in Ukraine are 1) The law of Ukraine "On the Fundamentals of National Resistance" and 2) Ukraine's reliance on drones in total defence strategy.

The first major enabler for drone accessibility is a legal framework to provide legitimacy and applicability to civilian resistance while staying faithful to democratic procedure (Fiala, 2023). In July 2021, Ukraine's President Zelenskyy signed the law "On the Fundamentals of National Resistance". This law permits involvement of Ukraine's citizens in support the nation's defence against adversarial aggression and occupation (Government of Ukraine, 2024). It created civil-military hierarchies and outlined authorities for civilians to directly participate in the war effort. For example, citizens may join the Territorial Defence Forces and augment the Armed Forces of Ukraine in direct action against occupation (Coleman, 2022). More broadly, the law provides governance in preparing citizens for national resistance by sustaining patriotic motivation and building practical skills for the defence of Ukraine (Government of Ukraine, 2024). Under this construct, Ukraine's government agencies provide educational resources to empower the civil populace for both passive and active resistance in support of and in collaboration with the Armed Forces of Ukraine (Government of Ukraine, 2022a). In summation, the authorities provided by the law "On the Fundamentals of National Resistance" leave imaginative citizens well poised to employ drones as a versatile tool supporting total defence so long as they stay within the legal bounds of legitimate resistance.

This civil-military cooperation complements our second major enabler specific to Ukraine: small drones as a mainstay of Ukraine's total defence strategy. Ukraine has invested heavily in drone tactics as an accessible and cost-effective alternative to resource constrained ammunition and precision weaponry (Kunertova, 2023a). To maximize their investment, Ukraine has relied on nonconventional practices for procuring and employing drones since the start of Russian occupation in 2014 (Chávez, Swed, 2023) and continues to do so with exponential progression. Within one day of Russia's full-scale invasion on Ukraine in 2022, the Ministry of Defence of Ukraine issued calls for individual citizens to donate their drones in defence of Kyiv (Government of Ukraine 2022b). By contrast, three years later, reports now claim that Ukraine domestically produced 2.2 million drones in 2024 and aims to increase output to 4.5 million drones in 2025 (Axe, 2025).

This massive scale of Ukraine's drone arsenal and usage creates a foundation for interoperability with tech savvy or enterprising civilians alike to participate in the war effort. The accessibility of drones on the civilian market and their versatility are only an asset so far as the primary warfighting institutions of the state allow. In the case of Ukraine, civilian drones are not a mere supplement to resistance. They are a foundational means for civilians to support total defence.

2. Empowered by Drones: An Individual Approach

Literature on civil resistance highlights that one of its inherent advantages is that it offers a low threshold for participation to those that otherwise would not have been voluntarily opted to engage in armed conflict (Bartkowski, 2013). This means civilian involvement in resistance can be incentivized by offering accessible means for individuals to support total defence. In this section, we will examine fundamental ways that individual civilians can interface with the war effort and specific qualities of drones that enable or amplify those efforts.

The broad categories we will examine for individual involvement in resistance are 1) resource contributions, 2) leveraging personal networks, and 3) developing and employing skills. Each of these categories provide opportunities to employ an individual civilian's personal qualities, assets, and political will towards resistance objectives in Ukraine.

2.1. Resource Contributions

Ukraine's war effort is driven in large part to external benefactors with over 250 billion dollars donated by the United States (Masters, Merrow, 2024) as EU (EU Delegation to the United States, 2024) combined as of 2024. However, it has also relied on internal efforts to pool resources from its own citizens for war materiel. This means, that in accordance with PRO-1, drone donations provide a means for civilians to *impose direct and indirect costs on an occupying force*.

Drones are uniquely suited to fulfil demands for war materiel due to their physical accessibility. They can be resourced, procured, or crafted by individual citizens. In the 'poor man's air force', individuals have the means to directly contribute airpower capabilities via commercial off-the-shelf drones or home-built designs (Hodson, 2024). These drones are regularly used in Ukraine for intelligence, surveillance, reconnaissance, artillery spotting, and as delivery devices for small explosives (Fiala, 2023). Every donated by a civilian has the potential to erode Russia's warfighting capacity and save Ukrainian lives when placed in the hands of a skilled operator.

These drones have also proven to be economically accessible means for civilians to contribute these capabilities (Jones, Kaczynski, Chávez, Edwards, 2024). From a cost standpoint, loitering munitions or kamikaze attack quadcopters cost hundreds or thousands of dollars rather than the hundreds-of-thousands dollar price point of modern munitions. Despite the price disparity, both categories produce similar effects on the battlefield (Kunertova, 2023b). Seasoned Ukrainian drone operators boast that cheap $2,000 drones can take out tanks that are worth millions (Melchior, 2023). This means civilians can impose outsized costs on the enemy by donating drones to Ukraine's front lines.

Moreover, Ukraine's citizens are not limited to the drones they can physically get their hands on through commercial means. They can simply contribute by donating cash to crowdfunding campaigns. By pooling resources, they can have a small stake in a larger drone that more closely mirror capabilities of a high-end military. For example, in the earliest days of the war, the People's Project campaign crowdsourced an advanced surveillance PD-1 drone and mobile command centre that cost a combined $36,750 (Jozuka, 2015). Additionally, by donating to organized crowdsource campaigns, Ukrainian citizens may also contribute to scaling smaller but standardized assets. This allows Ukraine's armed forces to field swarms of common assets for greater effect. For instance, in 2022, Ukraine solicited crowdfunding for its 'Army of Drones' initiative to fund 200 reconnaissance drones, thousands of civilian drones, and technical training for front line operators. The intent of this overall successful initiative was to provide constant coverage of its 2,470-kilometer front line with monitoring and rapid response capability (Kossov, 2022). These examples show how drones offer civilians low-risk and high impact means to *maintain popular support* in accordance with PRO-5.

We can extend this logic further when we consider blood donations as a means of *supporting* and *maintaining* the war effort. Demand for blood transfusion skyrocketed with the war and Ukraine's supply is constantly strained. Any Ukrainian aged 18 to 60 without any disqualifying conditions can donate blood (Ministry of Health of Ukraine, 2023). Drones have been for medical logistics to shuttle blood stockpiles between medical facilities such as in Bucha (Guz, 2023). Drones have even been as a lifeline for delivering blood bags directly to frontline trenches (Brizard, 2025). While this capability is largely in development, the application of drones for medical logistics can directly link civilian blood donations to saving lives of Ukrainian compatriots in regions of Ukraine where medical facilities are completely inaccessible or inoperable. We see yet again that drones can facilitate the low risk, yet lifesaving, endeavours of a supportive populace.

2.2. Leveraging Personal Networks

Ukraine's citizens that wish to contribute to the war effort are not limited to providing resources directly. Drones provide a common platform in the information space to *expand popular support*, i.e, PRO-5, and export political will to *external supporters,* i.e, PRO-2, by leveraging personal networks and social capital. An action as micro as forwarding a link on social media can expand support for a drone crowdfunding campaign and, therefore, the war effort. This simple act's magnitude of impact correlates to the size of one's audience and how influential their voice is to that audience. One prolific example: Ukrainian TV presenter, Serhiy Prytula, was able to crowdfund over twenty million dollars to purchase three Bayraktar drones to donate to Ukrainian war fighters (Kossov, 2022). Remarkably the company, Baykar Makina, opted to donate the drones outright with a request that the funds collected go towards supporting the people of Ukraine directly (Baykar, 2022). Another example of leveraging external star power is actor Mark Hamill's drone crowdfunding campaign which sourced 1,400 drones in three months (Government of Ukraine, 2022b). In both examples, we see the power of an individual's network amplifying both *popular* domestic and *external support* while marketing the role of drones as means to resist the oppressor.

Drones also provide additional 'ammunition' for individual civilians to directly engage in information warfare to *deny the occupier's political consolidation* i.e, PRO-3. The Ukrainian Resistance Pocketbook encourages civilians to produce and distribute propaganda with an emphasis on sharing accurate news (Government of Ukraine, 2022a). This line of effort is empowered by modern streaming cameras fitted to drones that provide battlefield videography on an unprecedented scale which is then proliferated through open sources. Drone videography of kinetic strikes, post-battle damage, and adversary war crimes are now in the hands of individual civilians. By propagating this footage on social media, Ukrainian civilians can inform their personal networks and the international community alike with shocking visuals directly from the front lines (Kunertova, 2023a). In doing so, they can also perpetuate *popular* and *external support* alike by pairing these visuals with their own personal narratives.

2.3. Developing and Employing Skills

Perhaps the most impactful way drones augment individual civilians is by providing an accessible platform for patriotic hobbyists and technicians alike to develop and employ their skills in support of the war effort. We've discussed how drones are physically accessible. However, the internet also provides limitless resources to build and modify drones at home. For example, a quick search on Amazon.com for 'drone delivery device' will display dozens of products that can weaponize a drone with a small explosive (Amazon, 2025). Furthermore, drone technicians with access to 3D printers can custom build, modify, and share blueprints that can be reproduced by other enthusiasts (*Inside Ukraine's DIY drone revolution*, 2023). The internet is abundant in how-to guides for building, modifying, and weaponizing drones. These techniques, tactics, and procedures are free and readily available on open-source resources like YouTube (Jones et al., 2024).

RAND researchers directly identified these technical drone skills as supporting PRO-1 *imposing direct or indirect costs* on Russian occupation forces by example of low-cost spotter drones (Kepe, Demus, 2023). In Ukraine, we see civilians with technical drone skills building, repairing, and employing these spotter drones to acquire targets for Ukrainian war fighters. In the words of one volunteer '…as the war becomes increasingly defined by artillery-on-artillery battles, the combined effect of spotter drones and the big guns is just as deadly' (Bellini, 2022).

Individual civilians that are trained and capable drone operators can also contribute directly to territorial defence during acute but critical moments of resistance. Drone informed civilians are empowered to alert Ukrainian authorities of enemy drone sightings. Ukraine's National Resistance Center has communication channels open for alerts as sighted drones may herald enemy artillery fire with only minutes to spare (Government of Ukraine, 2022c). Furthermore, while civilians are generally forbidden from flying drones in Ukrainian airspace, Ukraine's National Resistance Center outlines that there are times when civilians are able to supplement defence efforts with drones under the supervision of Ukraine's Armed Forces in the frontline or occupied territory

(Government of Ukraine, 2023). In this way, willing and capable drone operators can acutely *reduce the occupier's capacity to repress* their fellow citizens in accordance with PRO-3.

In each of the examples we've explored in this section, we see two trends that enable civilians to make individual contributions to resistance efforts. 1) Drones are physically, economically, and technologically accessible tools. 2) Drones provide accessible low risk means to support resistance activities. These findings are visualised below to connect these enablers to a versatile array of activities that support Ukraine's PROs.

Drone Enabled Activities in Support of Proximate Resistance Objectives (PROs)

	PRO-1: Imposing Direct or Indirect Costs on an Occupying Force	PRO-2: Securing External Support	PRO-3: Denying an Occupier's Political and Economic Consolidation	PRO-4; Reducing an Occupier's Capacity for Repression	PRO-5; Maintaining and Expanding Popular Support
Individual	• Donating drones (procure, resource or build) • Supplementing warfighters with technical skills	• Crowdfunding drones (leveraging networks) • Propagating drone videography	• Propagating drone videography	• Alerting authorities of drone sightings • Supplementing defense forces with technical skills	• Crowdfunding drones (contributing and leveraging networks) • Donating blood • Propagating drone videography

Versatility of applications

Accessibility as an enabler	1) Drones are physically, economically, and technologically accessible tools 2) Drones provide accessible low risk means to support resistance activities
Foundation:	1) Ukraine's Law "On the Fundamentals of National Resistance" 2) Drones as a mainstay of Ukraine's total defence strategy

Figure 1: Drone Enabled Activities in Support of PROs (Binnendjik, Kepe, 2021) at the Individual Level. Figure created by the author.

3. How Drones Drive Community War Efforts

As we have seen, drones enable individuals to interface with the war effort through resources, networks, and personal skills. However, we can most notably see Ukrainian activists leveraging these individual assets within group dynamics. These activities are typically 'spontaneous, need-based, and rely on existing informal networks at the community level' (Kepe, Demus, 2023). We will next explore how Ukraine's drone strategy capitalizes on these networks and empowers communities to band together to deliver effects with impact that outsize the sum of individual efforts. Three prominent means that we will examine briefly are 1) research and development, 2) information warfare and 3) building human capitol. As an overarching principle, these three means all inherently provide tailored and low risk opportunities to *increase participation and popular support* in accordance with PRO-5. However, we'll see how they also substantially advance other resistance objectives.

3.1. Research and Development

According to an advisor to the Ministry of Defence, Ukraine's approach to drone adaptation is deliberately nimble and has intentionally decentralized to avoid getting trapped in military bureaucracy (Melchior 2023). This diversified approach creates opportunities for enterprising drone technicians to rally and partner with Ukraine's defence forces to develop drone innovations for a rapidly evolving tactical environment. From as early as 2014, Ukrainian drone enthusiasts have collaborated in organized groups to build, modify, and field unmanned aerial vehicles in support of the war effort. These volunteer groups like Aerorovzvidka and People's Project compared themselves to Silicon Valley startups for warfighting (Chávez, Swed, 2023). They pride themselves in maintaining an agile adaptation cycle with new risks and developments in the tactical battlespace. For example, cheap DJI drones were a prominent improvised weapon system in earlier years of the war. When Russian combatants started using Aeroscope sensors in the DJI drones to track Ukrainians (DeVore, 2023), Aerorozvidka developed their own drones absent this major liability. These R18 octocopters also served as a hedge against DJI's outright ban on sales to Ukraine and Russia in 2022 as they protested their product's use in war (Radio Free Europe, 2022).

Drone garage-builds have become a community interest all throughout Ukraine. Armed with computers, 3D printers, virtual reality goggles, and the will to support their nation, hobbyists and professionals alike experiment on all manner of niche drone capabilities. Drone versatility allows communities to test different materials, payload capacities, range parameters, cameras, and artificial intelligence applications to find new asymmetric advantages for Ukraine and counter developments in Russia's drone tactics. Per the founder of underground drone manufacturer Airlogix 'Wherever you look in every garage, something is being made for the needs of the armed forces in the context of drones' (Schifrin, O'Connor, Goldman, 2024). In short, these garage-build drones have allowed Ukrainian warfighters to *impose outsized costs on the occupying force* by consistently delivering technological upgrades to the battlefield.

3.2. Information Warfare

Previously, open-source intelligence (OSINT) data was limited largely to mass media and government analysis. The recent advent of drone-provided battlefield footage provides open-source data on an unprecedented scale. This empowers civilians to provide a true picture on the ground to fight disinformation in line with the Resistance Operating Concept (Fiala, 2023). Now, communities of digital activists can complement professional news media because these OSINT practitioners are able to provide factual context for front line footage beyond the expertise of war reporters. Analysing each event can help the media build overarching narratives and combat false narratives that undermine the political will of Ukraine and the backing of its international partners (Freear, 2022). In other words, OSINT communities leverage drone footage to help preserve legitimacy of their government. According to the RAND PRO framework, this has the effect of *denying the occupier's political consolidation* (Kepe, Demus, 2023).

Furthermore, Ukraine's Resistance Pocketbook challenges civilians to 'Monitor occupiers systematically and document their atrocities to ensure they face justice' (Government of Ukraine, 2022a). In line with this charge and equipped with drone videography, this ecosystem of amateur journalists has evolved into an organised cadre of OSINT activists' intent on providing hard evidence of war crimes through 'web of accountability'. Dozens of these loose networks of activists are 'intricately linked with judicial authorities across the West and around the world' (Ricci, Crawford, 2025) and are able to scale judicial efforts at an accelerated rate based on drone-collected OSINT. These efforts aim to *secure external support* of judicial institutions and publicize atrocities with the intended aim of *reducing the occupier's capacity for repression*.

3.3. Building Human Capitol

Ukraine's appetite for drones by the millions (Axe, 2025) creates a requirement for a cadre of trained drone operators. Civilian private nongovernment organisations are providing this training to military and civilian drone pilots alike. One example is Dronarium which trains operators to fly and weaponize them on the battlefield. The founder claims the organization has trained thousands of pilots across all branches of Ukraine's armed forces (Nixon, 2024). Victory Drones is another non-governmental organisation that has partnered with Ukraine's armed forces. They offer a variety of courses aimed at defence professionals, supporting entities, and civilian enthusiasts in drone piloting, engineering, and volunteer instructor specialties. They even have a free course for service members to receive an accredited drone specialty within the military service (Victory Drones, 2024). These collective talent building initiatives can magnify the scale of drone operators that can further *impose costs on the occupier* and *reduce the occupier's capacity for repression,* as we've previously observed.

Through each of the activities we have examined, we can see how drones facilitate collaborative efforts in support of resistance. With these findings, we can map out and observe outsized effects these communities can have towards Ukraine's PROs.

Drone Enabled Activities in Support of Proximate Resistance Objectives (PROs)

Level of Actor	PRO-1: Imposing Direct or Indirect Costs on an Occupying Force	PRO-2: Securing External Support	PRO-3: Denying an Occupier's Political and Economic Consolidation	PRO-4; Reducing an Occupier's Capacity for Repression	PRO-5; Maintaining and Expanding Popular Support
Community	• Organizing drone donation drives and crowdfunds • Innovating "Garage builds" • Training drone technicians to supplement warfighters	• Organizing drone donation drives and crowdfunds • Documenting evidence of war crimes (OSINT)	• Preserving legitimacy and fighting disinformation (OSINT)	• Publicizing war crimes (OSINT) • Training drone technicians to supplement defense forces	• Organizing and expanding drone enabled communities
Individual	• Donating drones (procure, resource or build) • Supplementing warfighters with technical skills	• Crowdfunding drones (leveraging networks) • Propagating drone videography	• Propagating drone videography	• Alerting authorities of drone sightings • Supplementing defense forces with technical skills	• Crowdfunding drones (contributing and leveraging networks) • Donating blood • Propagating drone videography

Scalability of impact

Versatility of applications

Accessibility as an enabler	1) Drones are physically, economically, and technologically accessible tools 2) Drones provide accessible low risk means to support resistance activities 3) Drones facilitate collaborative efforts
Foundation:	1) Ukraine's Law "On the Fundamentals of National Resistance" 2) Drones as a mainstay of Ukraine's total defence strategy

Figure 2: Drone Enabled Activities in Support of PROs (Binnendjik, Kepe, 2021) at the Community Level. Figure created by the author.

4. Aggregating Drone Effects for Resistance at the National Level

To this point, we have discussed several effects that civilians have been able to deliver in support of total defence within their personal and professional means. Civilians can interface with drone equities in a technical capacity, in the information space, and the human domain in numerous ways. As these efforts coalesce and scale to the national level, we will see examples of how civilian use of drones delivers strategic effects in support of Ukraine's resistance when paired with a government-led total defence. The three ways we will examine are 1) strengthening political will, 2) building a drone industry, and 3) surging wartime readiness.

4.1. Strengthening Political Will

The Resisting Operating Concept emphasizes sustained national cohesiveness is a precondition for success in resistance. Involvement in non-governmental entities, such as those enabled by drones, is outlined as a means of promoting national identity (Fiala, 2020). One way to explain this is through Self-Perception Theory. This theory explains that individuals identify with attitudes, emotions, and attributes by observing their own behaviour (Bern, 1972). As we've seen, drones provide an accessible platform to interface with the war effort. This is in both direct ways like modifying drones but it's also in much subtler indirect ways like social media campaigns. In this way, drones lower the threshold of actions that a civilian can take while contributing to resistance goals which can perpetuate them to identify with and escalate those behaviours. When we examine the collaborative aspects of these activities through the lens of Social Identity Theory, we can see that these activists generally identify with the norms, values, identities and behaviours of the communities they've coopted themselves into (McLeod, 2023). When communities are oriented to protecting their nation, the individuals of those communities identify with those values. This means that the versatile spectrum of low-risk opportunities provided by drones can scale *popular support* through both individual actions, no matter how small, and affiliated community values.

Throughout the war, we've seen stories striving to sustain this patriotic will amongst a populace resisting aggression and occupation. For example, stories circulated in early 2022 about an ace pilot that shot down over 40 aircraft called the Ghost of Kyiv. The Ministry of Defence even forwarded a video over social media celebrating this mythic pilot. Later reports from the Ukrainian government confirmed the Ghost of Kyiv was solely a legend that was propagated for patriotic morale (Bingle, 2024). However, we've also seen real-life episodes where Ukraine's populace and government lionize heroics enabled by drones. This paper opened with one vivid account. The news story of Aerorozvidka operating halting a convoy juxtaposes their origins as drone hobbyists with their current role as vanguards of a 'David-and-Goliath' resistance (Borger, 2022). Another example directly is from the Ukrainian Government. The Hero of Chornobaivka is a volunteer who organized a group to track enemy combatants using drones at the start of Russia's full-scale invasion (Government of Ukraine, 2022d). Just like we saw in Mark Hammill's 'These are the drones you're looking for' crowdfund (Government of Ukraine, 2022b), drones are not framed as weapons of war in these stories. They are framed as a symbol of Ukraine's resistance.

4.2. Building a Drone Industry

In the words of Ukraine's Minister for Digital Transformation Mykhailo Fedorov 'this war is turning into a war of engineers and a war of economies. And whoever improves the level of development of their product will gain an advantage on the battlefield, will lose less people and will hit targets more effectively' (Schifrin et al., 2024).

The ambitions of Ukraine to develop and scale their drone employment relies heavily on its internal talent pool of talent: professional and hobbyist alike. Ukraine has pivoted many facets of their domestic economy to surging drone-making capacity in public-private partnerships. Ukraine's government visibly empowers this talent pool of drone communities to innovate technical solutions and adapt Ukraine's drone tactics on a rapidly changing battlefield. For example, Ukrainian workshops innovated drone modifications to conduct deep strikes on Russian oil facilities and aerodromes (DeVore, 2023) while they were constrained by political limitations placed on their missile arsenal. Russia's hierarchical drone development cycle and tactics, at least in the early stages of the war, do not appear to be so adaptive. (DeVore, 2023).

Furthermore, this talent pool allowed Ukraine's drone industry to multiply from seven domestic manufacturers to over eighty in 2023 alone (Thompson, 2024). Ukraine offers a unique testbed for every domestic enterprise producing military grade drones. Companies must stay ahead of the innovation curve on a rapidly evolving battlefield to stay relevant. This provides an imperative to leverage the homegrown talent pool of drone engineers and operators to accumulate lessons and deliver results to stay competitive. Deputy Minister of Defence of Ukraine, Dmytro Klimenkov, provided an updated estimate of 200 drone enterprises as of June 2024 and asserted that 'Almost 100% of all products are developed in Ukraine'. Most of these are private sector entities that directly contribute to Ukraine's war economy. The idea that Ukraine was a hotbed for Silicon Valley style startups has evolved into a narrative that Ukraine is becoming the world's epicentre for drone development. Ukraine's President Zelenskyy himself asserted 'Ukraine is now the world leader in drones' (Volodymyr Zelenskyy, 2025).

If we return to the PRO framework, we see that these civilian organizational partnerships scale resistance efforts to strategic level effects. The contributions of communities to Ukraine's thriving drone industry undoubtedly *imposes major costs on the occupying force* by producing millions of drones in support of total defence. In fact, a Royal United Services Institute report for assesses that tactical drones accounts for 60-70% of degraded or destroyed Russian systems as of early 2025 (Watling, Reynolds, 2025). Furthermore, it broadens Ukraine's *popular support* by providing opportunities to participate in total defence efforts on a massive scale through industry. Lastly, this decentralized drone industry *denies* Russia any concentrated means *to coopt and consolidate* Ukraine's *drone economy* within occupied territories.

4.3. Surging Wartime Readiness

In early 2024, President Zelenskyy issued a decree to stand up Unmanned Systems Force. Ukraine is now the first nation to have a dedicated service for air, land, and sea unmanned systems (Kushnir, 2024). The recruitment page is targeted towards individually technologically inclined citizens and outlines that the training pipeline is a remarkably short 17 to 40 days aided by partnerships with the private sector (Drone Force, 2024). While Unmanned Systems Force is new and still relatively undermanned, this initiative show how private communities can contribute human capital for Ukraine's armed forces by organizing, training, and equipping drone-inclined citizens in just a few weeks. In this way, drones provide a hedge against waning perceptions of more conventional military service routes. By comparison, infantry training operates on a similar timeline with a reputation for being too brief for the demands of an infantry fighter (Khurshudyan, Korolchuk, 2024). A drone operator trained in the same timeline can in theory utilize their craft to achieve a versatile range of effects: battlespace awareness, artillery spotting, loitering munitions, kamikaze strikes, war videographers, soldier evacuation, and medical resupply. Each of these operators becomes *capable of imposing direct costs on the occupiers* and *reducing occupier capacity for repression* while still minimizing time and resource investment.

Furthermore, under the law on national resistance, Ukraine's Territorial Defence Force has been able to train interested civilian volunteers to weaponize drones and directly supplement their warfighting effort (Lowther, Siddiki, 2022). This creates an ad hoc force equipped to drop Molotov cocktails against occupiers or to directly back frontline soldiers in critical periods. The world saw this in practice during the Battle of Kyiv in 2022. During this precipitous battle, local resisting civilians used drones to identify inbound enemy tanks, guided indirect fire barrages, and delivered loitering munitions on enemy positions in tandem with the Ukrainian armed forces. Their efforts helped Ukraine win arguably one of the most pivotal battles in modern history (Marson, 2022) which further contributes to the inspired stories that expand Ukraine's will to resist.

Our final iteration of our recurring map of PROs scales drone enabled activities to the national level. Here we can see exactly how drones empower civilians in resistance at every level. The accessible and versatile nature of drones in Ukraine enables civilians to act in support of all lines of PROs. These efforts are compounded by drones' ability to scale and deliver strategic effects towards the nation's total defence.

Drone Enabled Activities in Support of Proximate Resistance Objectives (PROs)

Level of Actor	PRO-1: Imposing Direct or Indirect Costs on an Occupying Force	PRO-2: Securing External Support	PRO-3: Denying an Occupier's Political and Economic Consolidation	PRO-4; Reducing an Occupier's Capacity for Repression	PRO-5; Maintaining and Expanding Popular Support
National	• Growing defense industry • Surging drone production • Innovating drone solutions to evolving battlespace • Surging human capitol for warfighting	• Providing allies means to support with resources and amplify narratives	• Decentralizing defense industrial base	• Surging human capitol for homeland defence	• Building national identity via community activities • Strengthening patriotic will via drone heroics • Expanding opportunities to contribute to total defence
Community	• Organizing drone donation drives and crowdfunds • Innovating "Garage builds" • Training drone technicians to supplement warfighters	• Organizing drone donation drives and crowdfunds • Documenting evidence of war crimes (OSINT)	• Preserving legitimacy and fighting disinformation (OSINT)	• Publicizing war crimes (OSINT) • Training drone technicians to supplement defense forces	• Organizing and expanding drone enabled communities
Individual	• Donating drones (procure, resource or build) • Supplementing warfighters with technical skills	• Crowdfunding drones (leveraging networks) • Propagating drone videography	• Propagating drone videography	• Alerting authorities of drone sightings • Supplementing defense forces with technical skills	• Crowdfunding drones (contributing and leveraging networks) • Donating blood • Propagating drone videography

Scalability of impact

Versatility of applications

Accessibility as an enabler	1) Drones are physically, economically, and technologically accessible tools 2) Drones provide accessible low risk means to support resistance activities and facilitate collaborative efforts 3) Drones facilitate collaborative efforts
Foundation:	1) Ukraine's Law "On the Fundamentals of National Resistance" 2) Drones as a mainstay of Ukraine's total defence strategy

Figure 3: Drone Enabled Activities in Support of PROs (Binnendjik, Kepe, 2021) at the National Level. Figure created by the author.

Conclusion

Drone use in Ukraine provides a vivid case study in how an emerging technology can empower individuals to directly contribute effects in support of total defence. To understand the dynamics of Ukraine's resisting populace, this research paper sought to answer the question: **How do drones uniquely empower Ukraine's civilians to contribute to national resistance against Russian occupation?**

By examining the unique properties that drones can provide in the context of Ukraine's total defence, we have determined that there are three overarching qualities that make drones uniquely suited for civilians to advance resistance objectives. This paper concludes that **Ukraine's resistance to Russian occupation demonstrates that drones can uniquely empower civilians by providing accessible, versatile, and scalable means to contribute to total defence.**

Of note, the major limitation of this exploratory research is that it primarily focuses on how drones *empower* civilian resistance. This means it is inherently biased towards positive aspects of the unmanned systems. Given that drones are emerging technology, there will be unforeseeable second or third order effects in this relatively new relationship between state-sponsored civilian resistance and drone technology. There may also be new ways this relationship emboldens civilians in the future that have yet to even be conceptualized. Therefore, this author recommends continued research on the long-term second and third order effects of state-sponsored drone diffusion in Ukraine as those effects become more apparent.

Lastly, two foundational pre-conditions for drone enabled resistance were established in Ukraine: 1) a resistance legal framework and 2) drones as a mainstay of total defence. This author recommends researchers and policy makers consider how other resistance-oriented states could create accessible conditions for drones to maximize their potential within that geopolitical context.

Bibliography

AMAZON. 2025. Amazon.com search “drone delivery device.” [Online]. 1 March 2025. [Cited : 1 March 2025]. https://www.amazon.com/s?k=drone+delivery+device&crid=3UL1OSGLKRRM8&sprefix=drone+delivery+device%2Caps%2C176&ref=nb_sb_noss_1

AXE, David. 2025. 4.5 Million Drones Is A Lot Of Drones. It’s Ukraine’s Goal For 2025. *Forbes*. [Online]. 12 March 2025. [Cited : 22 March 2025]. https://www.forbes.com/sites/davidaxe/2025/03/12/45-million-drones-is-a-lot-of-drones-its-ukraines-new-production-target-for-2025/

BARTKOWSKI, Maciej J. (ed.). 2013. *Recovering nonviolent history: civil resistance in liberation struggles*. Boulder, Colorado: Lynne Rienner Publishers, Inc. ISBN 978-1-58826-870-9.

BAYKAR. 2022. Announcement from Baykar. *Twitter*. [Online]. 27 June 2022. [Cited : 6 January 2025]. https://x.com/BaykarTech/status/1541478839662043136

BELLINI. 2022. Ukrainian Civilians Use Drones To Help Fight Against Russian Forces. *Scripps News*. [Online]. 3 May 2022. [Cited : 1 March 2025]. https://www.scrippsnews.com/world/ukrainian-civilians-use-drones-to-help-fight-russia

BERN, Daryl J. 1972. Self-Perception Theory. In: *Advances in Experimental Social Psychology*. [Online]. Elsevier. pp. 62. [Cited : 1 March 2025]. ISBN 978-0-12-015206-3.

BINGLE, Morgan. 2024. Information Warfare & the Ghost of Kyiv. *The Henry M. Jackson School of International Studies*. [Online]. 12 February 2024. [Cited : 1 March 2025]. https://jsis.washington.edu/news/information-warfare-the-ghost-of-kyiv/

BINNENDJIK, Anika and KEPE, Marta. 2021. *Civilian-Based Resistance in the Baltic States: Historical Precedents and Current Capabilities* [Online]. RAND Corporation. [Cited : 1 March 2025].

BORGER, Julian. 2022. The drone operators who halted Russian convoy headed for Kyiv. *The Guardian*. [Online]. 28 March 2022. [Cited : 12 December 2024]. https://www.theguardian.com/world/2022/mar/28/the-drone-operators-who-halted-the-russian-armoured-vehicles-heading-for-kyiv

BRIZARD, Lucille. 2025. Azov Medics Use Drone to Deliver Blood in Battlefield Rescue Under Fire, Video. *UNITED24 Media*. [Online]. 4 March 2025. [Cited : 20 March 2025]. https://united24media.com/latest-news/azov-medics-use-drone-to-deliver-blood-in-battlefield-rescue-under-fire-video-6425

CHÁVEZ, Kerry and SWED, Ori. 2023. Emulating underdogs: Tactical drones in the Russia-Ukraine war. *Contemporary Security Policy*. 2 October 2023. Vol. 44, no. 4, pp. 592–605. DOI 10.1080/13523260.2023.2257964.

COLEMAN, Julie. 2022. “Putin should be afraid of us”: Regular Ukrainian civilians are training to fight off a Russian invasion. *Business Insider*. [Online]. 1 February 2022. [Cited : 12 December 2024]. https://www.businessinsider.com/regular-ukrainian-civilians-are-training-for-conflict-with-russia-2022-2

DEVORE, Marc R. 2023. “No end of a lesson:” observations from the first high-intensity drone war. *Defense & Security Analysis*. 3 April 2023. Vol. 39, no. 2, pp. 263–266. DOI 10.1080/14751798.2023.2178571.

DRONE FORCE. 2024. Drone Force - The project to recruit unmanned systems specialists. [Online]. 2024. [Cited : 11 December 2024]. https://landforces.mil.gov.ua/df

EU DELEGATION TO THE UNITED STATES. 2024. EU Assistance to Ukraine (in U.S. Dollars) | EEAS. [Online]. 23 September 2024. [Cited : 9 December 2024]. https://www.eeas.europa.eu/delegations/united-states-america/eu-assistance-ukraine-us-dollars_en?s=253

FIALA, Otto C. 2020. *Resistance Operating Concept (ROC)*. MacDil Air Force Base, Florida. ISBN 978-1-941715-43-7.

FIALA, Otto C. 2023. Resilience and Resistance in Ukraine. *Small Wars Journal by Arizona State University*. [Online]. 1 January 2023. [Cited : 11 December 2024]. https://smallwarsjournal.com/2023/01/01/resilience-and-resistance-ukraine/

FREEAR, Matt. 2022. OSINT in an Age of Disinformation Warfare. *Royal United Services Institute*. [Online]. 14 March 2022. [Cited : 12 December 2024]. https://rusi.orghttps://rusi.org

GOVERNMENT OF UKRAINE. 2022a. *Ukrainian Resistance Pocketbook.* [Online]. 2022. [Cited : 11 December 2024]. https://drive.google.com/file/d/1Sm1VjtQsXrQCf3o8h71Tr_2uiMkaG4HL/view

GOVERNMENT OF UKRAINE. 2022b. These are the drones you're looking for: Join Mark Hamill and the Army of Drones. [Online]. September 2022. [Cited : 11 December 2024]. https://u24.gov.ua/dronation

GOVERNMENT OF UKRAINE. 2022c. Hunting for an eagle: What to do if you spot a Russian drone. *National Resistance Center of Ukraine*. [Online]. 4 August 2022. [Cited : 12 December 2024]. https://sprotyv.mod.gov.ua/polyuvannya-na-orlana-shho-robyty-yakshho-pomityly-rosijskyj-bezpilotnyk/

GOVERNMENT OF UKRAINE. 2022d. Heroes of the resistance. How underground helped to destroy the enemy in Chornobayivka. *National Resistance Center of Ukraine*. [Online]. 1 December 2022. [Cited : 8 January 2025]. https://sprotyv.mod.gov.ua/en/heroes-of-the-resistance-how-underground-helped-to-destroy-the-enemy-in-chornobayivka/

GOVERNMENT OF UKRAINE. 2023. How to properly track the enemy using drones/quadcopters. *National Resistance Center of Ukraine*. [Online]. 27 April 2023.

[Cited : 12 December 2024]. https://sprotyv.mod.gov.ua/yak-pravylno-zdijsnyuvaty-stezhennya-za-vorogom-za-dopomogoyu-droniv-kvadrokopteriv/

GOVERNMENT OF UKRAINE. 2024. Law of Ukraine: On the foundations of national resistance. *Official website of the Parliament of Ukraine*. [Online]. 20 June 2024. [Cited : 11 December 2024]. https://zakon.rada.gov.ua/go/1702-20

GUZ, Ulyana. 2023. Solutions from Ukraine: Bucha introduces drone delivery of medicine to medical institutions. *Rubryka*. [Online]. 30 July 2023. [Cited : 6 January 2025]. https://rubryka.com/en/2023/07/30/u-buchi-drony-dostavlyatymut-liky-do-medzakladiv-u-chomu-rishennya/

HODSON, Ryan. 2024. The Weaponisation of Toys and Implications for the Air Force. *Air and Space Power Centre*. [Online]. 9 September 2024. [Cited : 1 March 2024]. https://airpower.airforce.gov.au/blog/weaponisation-toys-and-implications-air-force

Inside Ukraine's DIY drone revolution, 2023. [Online]. [Cited : 1 March 2025]. https://www.youtube.com/watch?v=5vmuObO0vNk

JONES, Laura, KACZYNSKI, Nathan, CHÁVEZ, Kerry and EDWARDS, Bill. 2024. Drones are Here to Stay: The Proliferation of Unmanned Aerial Systems Across the Spectrum of War. *Irregular Warfare Initiative*. [Online]. 27 June 2024. [Cited : 1 March 2025]. https://irregularwarfare.org/podcasts/drones-are-here-to-stay-the-proliferation-of-unmanned-aerial-systems-across-the-spectrum-of-war/

JOZUKA, Emiko. 2015. A Crowdfunded UAV Is Helping Ukraine's Bootstrapped Army. *Vice*. [Online]. 18 June 2015. [Cited : 11 December 2024]. https://www.vice.com/en/article/a-crowdfunded-uav-is-helping-ukraines-bootstrapped-army/

KEPE, Marta and DEMUS, Alyssa. 2023. *Resisting Russia: Insights into Ukraine's Civilian-Based Actions During the First Four Months of the War in 2022* [Online]. RAND Corporation. [Cited : 1 March 2025].

KHURSHUDYAN, Isabelle and KOROLCHUK, Serhii. 2024. Basic training in Ukraine is barely covering the basics, commanders say. *Washington Post*. [Online]. 2 June 2024. [Cited : 8 January 2025]. https://www.washingtonpost.com/world/2024/06/02/ukraine-training-soldiers-mobilization-war/

KOSSOV, Igor. 2022. A Game of Drones: Ukraine builds up UAV fleet. *The Kyiv Independent*. [Online]. 26 July 2022. [Cited : 11 December 2024]. https://kyivindependent.com/a-game-of-drones-ukraine-builds-up-uav-fleet/

KUNERTOVA, Dominika. 2023a. The war in Ukraine shows the game-changing effect of drones depends on the game. *Bulletin of the Atomic Scientists*. 12 March 2023. Vol. 79, no. 2, pp. 95–102. DOI 10.1080/00963402.2023.2178180.

KUNERTOVA, Dominika. 2023b. Drones have boots: Learning from Russia's war in Ukraine. *Contemporary Security Policy*. 2 October 2023. Vol. 44, no. 4, pp. 576–591. DOI 10.1080/13523260.2023.2262792.

KUSHNIR, Natalia. 2024. As Ukraine focuses on drone warfare, its military creates new Unmanned Systems Forces branch. *ABC News*. [Online]. 12 June 2024. [Cited : 8 January 2025]. https://abcnews.go.com/International/ukraine-focuses-drone-warfare-military-creates-new-unmanned/story?id=111046806

LOWTHER, Adam and SIDDIKI, Makhbube. 2022. Combat Drones in Ukraine. *Air & Space Operations Review*. Winter 2022. Vol. 1, no. 4, pp. 3–13.

MARSON, James. 2022. The Ragtag Army That Won the Battle of Kyiv and Saved Ukraine. *Wall Street Journal*. [Online]. 20 September 2022. [Cited : 7 January 2025]. https://www.wsj.com/articles/russian-invasion-ukraine-battle-of-kyiv-ragtag-army-11663683336

MASTERS, Jonathan and MERROW, Will. 2024. How Much U.S. Aid Is Going to Ukraine? *Council on Foreign Relations*. [Online]. 27 September 2024. [Cited : 9 December 2024]. https://www.cfr.org/article/how-much-us-aid-going-ukraine

MCLEOD, Saul. 2023. Social Identity Theory In Psychology (Tajfel & Turner, 1979). *Simple Psychology*. [Online]. 5 October 2023. [Cited : 1 March 2025]. https://www.simplypsychology.org/social-identity-theory.html

MELCHIOR, Jillian Kay. 2023. Drones Are Giving Ukraine a Wartime Edge. [Online]. 23 February 2023. [Cited : 12 December 2024]. https://www.wsj.com/articles/drones-are-giving-ukraine-a-wartime-edge-homemade-dji-china-russia-tanks-weaponry-invasion-civilian-volunteer-russian-occupation-5c0bab55

MINISTRY OF HEALTH OF UKRAINE. 2023. Your Blood Can Fight! *Lviv Regional Center for Disease Control and Prevention of the Ministry of Health of Ukraine*.

[Online]. 14 June 2023. [Cited : 6 January 2025]. https://www.cdc.lviv.ua/post/твоя-кров-може-воювати

NIXON, Geoff. 2024. Drones are key in Ukraine's fight against Russia. Now it wants 1 million more of them. *CBC News*. [Online]. 3 March 2024. [Cited : 12 December 2024]. https://www.cbc.ca/news/world/ukraine-1-million-drones-russia-war-1.7130368

O'GRADY, Siobhán and KHUDOV, Kostiantyn. 2024. As Ukraine runs low on ammo, civilians build troops DIY drones at home. *Washington Post*. [Online]. 28 April 2024. [Cited : 12 December 2024]. https://www.washingtonpost.com/world/2024/04/28/ukraine-runs-low-ammo-civilians-build-troops-diy-drones-home/

PANELLA, Chris. 2023. The world is watching the war in Ukraine through drones, and it twists the view of who is winning this fight. *Business Insider*. [Online]. 30 December 2023. [Cited : 12 December 2024]. https://www.businessinsider.com/drone-footage-in-ukraine-twists-perception-of-the-war-shows-2023-12

RADIO FREE EUROPE. 2022. Drone Wars: Ukraine's Homegrown Response To "Deadly" Chinese Detection Tech. [Online]. 14 July 2022. [Cited : 11 December 2024]. https://www.rferl.org/a/drone-detection-war-ukraine-china-russia/31943191.html

RICCI, Andrea and CRAWFORD, Jack. 2025. Puzzling Pieces: OSINT and War Crime Accountability in Ukraine. *Puzzling Pieces: OSINT and War Crime Accountability in Ukraine*. [Online]. 6 January 2025. [Cited : 26 September 2024]. https://rusi.orghttps://rusi.org

SCHIFRIN, Nick, O'CONNOR, Eric and GOLDMAN, Nikol. 2024. How drone warfare has transformed the battle between Ukraine and Russia. *PBS News*. [Online]. 16 January 2024. [Cited : 11 December 2024]. https://www.pbs.org/newshour/show/how-drone-warfare-has-transformed-the-battle-between-ukraine-and-russia

THOMPSON, Kristen. 2024. How the Drone War in Ukraine Is Transforming Conflict | Council on Foreign Relations. *Council on Foreign Relations*. [Online]. 16 January 2024. [Cited : 12 December 2024]. https://www.cfr.org/article/how-drone-war-ukraine-transforming-conflict

VICTORY DRONES. 2024. Victory Drones. Strengthening the technological capabilities of the Defense Forces. [Online]. 2024. [Cited : 11 December 2024]. https://en.victory-drones.com

VOLODYMYR ZELENSKYY. 2025. X Post from Volodymyr Zelenskyy. *Twitter*. [Online]. 15 February 2025. [Cited : 1 March 2025]. https://x.com/ZelenskyyUa/status/1890750796347875359

WATLING, Jack and REYNOLDS, Nick. 2025. *Tactical Developments During the Third Year of the Russo–Ukrainian War*. London, United Kingdom: Royal United Services Institute for Defence and Security Studies.

MAJ Egidijus Ciulada. What are Joint Command and General Staff Course students' perceptions of mission command?

Introduction

Col. J. R. Boyd claims that ‘give lower-level commanders wide freedom, with an overall mind time space scheme, to shape/ direct their own activities so that they can exploit faster tempo/ rhythm at tactical levels yet be in harmony with larger pattern/ slower rhythm associated with the more general aim and larger effort at the strategic level’ (Boyd, 2007).

In modern days, mission command as a command philosophy is considered the most suitable for wars and military operations. Initially, this philosophy was devised by the Prussians to mitigate the consequences of friction in war and is known as *Auftragstaktik* (Ben-Shalom, et. al., 2011). In the United States Army doctrine publication 6-0 (Mission Command), this philosophy is expressed as an application of authority and directions by the commander using mission orders that facilitate disciplined initiative inside the commander’s intent to empower adaptable and flexible leaders in the execution of unified land operations (ADP, 2012). Moreover, during the Professional Military Education in the Baltic Region 1919-2024 conference, Baltic Defence College commandant Brigade General Alvydas Siuparis said that each student has a different perception of mission command (Siuparis, 2024). Military education institution Baltic Defence College organise the Joint Command and General Staff Course (JCGSC) and prepares future officers for the highest levels of leadership. Therefore, understanding the perceptions of JCGSC students regarding mission command might be essential to assess its effectiveness and identify areas for improvement.

This research paper explores JCGSC students' perceptions regarding mission command. By understanding their views, one gains useful insights into the strengths and weaknesses of current mission command practices, helping to identify areas for further development and valuable information on how well military education prepares these students for applying mission command principles in dynamic and unpredictable military scenarios. The paper will examine the following research questions: how does theoretical understanding shape JCGSC students' perception of mission command; what role does practical experience play in influencing their perception; are there discernible differences in perception between students with more versus less field experience? To answer this question, the paper will review existing literature on mission command and interviews will be conducted to obtain qualitative data to be analysed for deeper insights into individual JCGSC student experiences and perceptions.

The findings of this research will contribute to a better understanding of mission command and its implementation in military organisations. By identifying areas where JCGSC students perceive gaps or challenges, the paper can provide recommendations for improving mission command practices and enhancing military leadership effectiveness. This paper will argue that the JCGSC student's perception of mission command is influenced by their gained theoretical understanding and practical experiences in the military career.

Mission command philosophy

The evolution of mission command, which is primarily based on the Prussian notion of *Auftragstaktik*, represents a significant change towards decentralisation in military command, encouraging adaptation and initiative. Fundamentally rooted in the idea of *Auftragstaktik*, which began in the Prussian army reforms following the terrible losses at Jena and Auerstedt in 1806, is the historical growth of mission leadership. This approach stresses distributed command, enabling subordinates to operate in line with the commander's objectives and promote initiative and flexibility on the battlefield (Sonnenberger, 2013). Major military conflicts in the 20th century, such as the First and Second World Wars, have shown that the traditional, strictly hierarchical command model is too rigid for the rapidly changing conditions on the battlefield (King, 2017).

This has led to the search for alternative models of leadership, of which mission command stands out, emphasising the ability of leaders to adapt to the situation and to act autonomously under shared goals rather than rigid orders; for example, the Swedish Armed Forces are adapting the methods of goal-based leadership to better prepare for future challenges (Nilsson, 2021). This evidence illustrates the growing importance of decentralised command structures, which encourage autonomous decision-making and strategic agility in combat situations. As modern warfare becomes increasingly complex, these flexible approaches offer a distinct advantage over traditional models. Mission command's historical roots and current relevance highlight its vital role in modern military strategy, however a combination of different leadership styles can limit or accelerate mission command to accomplish operational goals.

Mission command is an essential part of modern military leadership, requiring a focus on training to effectively address the complexities of modern combat, asymmetric threats and unconventional warfare through flexibility and autonomy. The importance of such a command type was particularly evident during the Cold War when the need to address asymmetric threats and unconventional warfare arose. It has become necessary to respond flexibly to modern military situations where rapid, autonomous decisions are required (Ploumis, 2020). Modern warfare, characterised by rapid technological advances and changing threat types, requires not only operational leadership but also the developed trust of commanders in subordinates. The implementation of mission command leadership ensures that leaders not only make quick decisions but also foster independent thinking among subordinates, thus contributing to greater effectiveness on the battlefield (Vandergriff, 2019). In addition, the importance of training in developing leaders' competencies is increasingly emphasised. Professional training of officers plays an important role in developing leaders who can act under the principles of mission command (Murray, 2014). Meanwhile, the US Army Doctrine ADP 6-0 and NATO Doctrine AJP-01 principles emphasise that this model of leadership is based on trust and freedom of decision-making, encouraging adaptation and innovation in all branches of military leadership (ADP 6-0, 2012 and AJP 0-1, 2022). It shows that mission command improves military effectiveness by fostering autonomy and creativity, especially in quickly changing combat scenarios. Training enables leaders to apply these ideas to real-world issues, ensuring they can maintain operational control while empowering subordinates. Mission command highlights the importance of today's army command, emphasising the need for training to handle the intricacies of current military operations.

The US Doctrine ADP 6-0 and NATO Doctrine AJP 0-1 share the same idea of command philosophy but are described differently. US Doctrine ADP 6-0 identifies that a leader's direction shapes team development and promotes mutual trust and common understanding; while encouraging freedom of activity and initiative, leaders provide resources and offer a clear aim that directs subordinates' activities (ADP 6-0, 2012). NATO Doctrine AJP 0-1 highlights that the foundations of trust and mutual understanding direct successful mission command (AJP 0-1, 2022). Both Doctrines principles are defined in the table (see Table 1). ADP 6-0 and AJP-01 mission command concepts are similar in emphasising decentralisation, flexibility, and trust. Both approaches prioritise decentralised execution, encouraging subordinates to operate following the commander's objectives to develop flexibility and initiative. Similarly, they emphasise the significance of rapid decision-making to adapt to changing surroundings and to sustain operational performance. However, they differ in framing. ADP 6-0 focuses on forming cohesive teams via mutual trust and shared understanding as essential characteristics, whereas AJP-01 focuses on unity of effort within multinational coalitions, addressing the complexities of integrating varied players and resources. Furthermore, ADP 6-0 specifically emphasises taking sensible risks and employing mission orders to direct operations, which are not as explicit in AJP-01 principles but are implied in its emphasis on decentralised and coordinated activity. These distinctions reflect the US Army's focus on internal cohesiveness and trust-building instead of NATO's emphasis on multilateral coherence. Understanding these contrasts makes it essential for military leaders to manage joint operations, ensuring that the capabilities of each doctrine are maximised for an integrated and comprehensive approach to mission command.

No.	The US Army Doctrine ADP 6-0	NATO Doctrine AJP-01
1.	Build cohesive teams through mutual trust (two-way communication, leadership, and shared experiences help to create mutual trust).	Unity of effort (ensures that activities are aligned at all levels, resulting in coherence in multinational operations).
2.	Create shared understanding (through cooperation and communication, define the operating environment and goals in common sense).	Timely and effective decision-making (encourages adaptability in responding to changing operational conditions).
3.	Provide a clear commander's intent (to direct subordinates' actions, clearly describe the aim, the key tasks, and the end state of the task).	Decentralised execution (subordinates are empowered to make decisions within their commander's intent, encouraging initiative and flexibility).
4.	Exercise disciplined initiative (under the commander's intent to respond to changing circumstances, subordinates act independently and prudently).	
5.	Use mission orders (highlight the results to be attained instead of dictating how to get them, therefore giving room for adaptation and flexibility).	
6.	Accept prudent risk (commanders must proactively expose their soldiers to risk when the prospective favour permits it, avoiding unneeded exposure to danger).	

Table 1. Principles defined by the US Army doctrine ADP 6-0 and NATO doctrine AJP-01 (ADP 6-0, 2012 and AJP-01, 2022)

Mission command and direct command are contrasting leadership styles in military operations. The direct command leadership style is defined as a leadership style where defining tasks, setting goals, and monitoring progress are required (Wong, et. al., 2003). In this type of command, the commanders are responsible for issuing detailed mission orders that outline the execution of the operation and its intended results. Furthermore, subunits are supposed to notify headquarters of any changes, allowing their commanders to respond in a timely manner (Ben-Shalom, et. al., 2011). In contrast, mission command encourages commanders to act autonomously on the basis of shared objectives, which allows them to react more quickly to unexpected challenges and adapt to the environment (Shamir, 2011). While direct command provides predictability and order, it may limit response in dynamic settings. In contrast, mission command's emphasis on autonomy and trust improves adaptability and rapid reaction to challenges. Understanding these differences highlights the importance of selecting appropriate leadership models for varying military contexts.

Through different focuses, mission command and transformational leadership represent two leadership styles that share common principles. As outlined before, mission command emphasises decentralised decision-making and operational autonomy, allowing subordinates to operate autonomously while sticking to the commander's intent. Similarly, transformational leaders affect some traits of the follower, such as empowerment, commitment, self-efficacy beliefs, job satisfaction, trust, and motivation (Givens, 2008). Transformational leadership further distinguishes itself by motivating followers via a common vision, promoting ethical behaviour, and addressing individual needs to generate long-term, meaningful change (Freund, 2019). Vesa Nissinen emphasises the significance of adapting leadership styles to organisational demands, as well as the relevance of values and ethical concerns in military leadership, which are consistent with transformational leadership ideas (Nissinen, 2001). Mission command promotes operational autonomy and agility, making it vital in dynamic and decentralised contexts. In contrast, transformational leadership focuses on developing moral behaviour and creating long-term change, assuring an organisation's sustainability and coherence. Although empowerment is essential for both leadership approaches, they can complement each other in their applications. Military organisations can evaluate their specific requirements and employ both forms of leadership that not only accomplish operational goals but also foster an ethical and cohesive atmosphere in the units. While these approaches serve separate purposes, they are comparable in their application.

Mission command and professional military education

Mission command, a form of decentralised leadership, must have a solid theoretical basis to be applied appropriately. In Nicholas Murray's analysis of professional military education (PME) he asserts that theoretical frameworks are essential in the process of establishing mission command within the military culture. Murray believes that critical thinking, which is achieved through an appropriate curriculum, helps military commanders understand the command intent and act with innovation when conducting operations (Murray, 2014). Likewise, Vandergriff stresses that leaders should first comprehend the concept of mission command, meaning that an ineffective understanding of the theoretical framework is associated with inconsistent and shallow practice (Vandergriff, 2019). Such statements of the importance of education in the learning and practising of mission command are quite evident.

However, there is still a way to improve the effectiveness of the training in PME programs. Murray critiques the emphasis on rote learning and limited engagement with critical thinking, which he believes undermines the development of independent decision-making skills (Murray, 2014). Vandergriff agrees with this by pointing out the fact that the existing training mechanisms do not challenge the students to the level where they can think critically or develop the kind of flexibility that is needed for adaptive leadership (Vandergriff, 2019). This discrepancy raises concerns about how effective PME is in readying students for the conversion of theory into reality, especially when they are faced with the complexities and constraints of real-world operations.

Practical experience is one of the most important factors that influence military students' perception of mission command. As Murray notes, the principle of mission command is closely associated with real-world applications during which the leaders have to make autonomous decisions when there is a lack of information (Murray, 2014). Vandergriff expands on this by arguing that experiential learning is the key to closing the gaps between academic learning and operational realities (Vandergriff, 2019). Those leaders who have been through situations where life was at stake are usually in a better position to understand the benefits of decentralised command, as their practical examples prove the effectiveness of this approach. Although experience has been recognised as an important factor, the implementation of practical learning in PME has not been coherent. Murray pointed out that PME has a lot of hours devoted to training mission command, but only a small portion of these hours includes scenarios that challenge students' critical thinking and decision-making (Murray, 2014). Similarly, Vandergriff criticises the traditional training model and promotes the use of simulations and realistic scenarios based on the complexities of modern warfare (Vandergriff, 2019). This tension indicates that while practical experience is necessary, its role in the students' understanding of mission command depends on how well the PME systems replicate the operational environment.

The connection between practical experience and the perception of mission command is not that simple because there are differences in students' operational backgrounds. According to Vandergriff, students who have had more operational exposure are more likely to internalise mission command since their experiences underline the importance of initiative and confidence in decentralised operations (Vandergriff, 2019). As noted, Murray PME programs receive students with diverse operational backgrounds; some students may have several years of experience in the field, while others are in the early stages of their careers (Murray, 2014). This variation provides a dynamic learning environment but, at the same time, poses challenges in standardising educational outcomes. Conversely, students with limited experience can find it challenging to connect the theoretical knowledge they are learning and the real-world applications. Murray emphasises that these students usually lack the contextual understanding needed to understand the intricacies of mission command (Murray, 2014). Vandergriff suggests that this gap can be filled by the use of mentorship and peer learning in which the more experienced leaders share their insights and lessons from the field (Vandergriff, 2019). However, this approach has its drawbacks as it is based on the willingness and ability of experienced students to contribute effectively to the learning environment. And even more so on the idea of how theory differs from practical knowledge.

While both Murray and Vandergriff offer important findings on the role of PME and practical experience in understanding mission command, several gaps were identified in the current literature. First, neither author fully addresses how PME curricula can be structured to meet the needs of students with different levels of experience. This may lead to the continuation of disparities in the achievement of learning outcomes, with the less experienced students not being able to achieve the same level of competency as the students who are experienced. Secondly, there is a need to explore how cross-cultural and joint-force dynamics influence mission command perceptions in more detail. This is important as modern military operations are characterised by multinational and interagency cooperation; understanding these dynamics is crucial for building the ability of leaders to operate in diverse environments. Lastly, both authors discuss the weaknesses of the current training models; however, their arguments are mainly based on theoretical perspectives and there is no sufficient empirical evidence to support their claims.

The relationship between theoretical understanding, practical experience, and individual backgrounds significantly influences how military students understand and execute mission command. While Murray and Vandergriff strongly critique present PME methods, their findings underscore the importance of a more nuanced approach to education and training. This also stresses the need to reevaluate how the teaching body conducts modern military training and their military background – either theoretical or operational – and how those clash with the PME expectations.

Further, the paper will investigate the empirical aspects of the appliance and understanding of the mission command within the PME. Starting with the chosen methodology.

Research methodology

Today’s military operations require a leadership model that harmonises decentralisation with strategic coherence. Mission command, based on the ideas of trust, autonomy, and adaptability, has become an essential strategy for managing dynamic and uncertain environments. Moreover, the link between theoretical knowledge, practical experience, and individual backgrounds has an impact on how military students understand and carry out mission command, as described in the first and second chapters. In 2024, seventy-six officers from fifteen countries attended the JCGSC in Baltic Defence College from fifteen NATO and Ally countries with different backgrounds and experiences to improve their leadership abilities. This chapter describes the research methodology and participants' characteristics to better understand students' perceptions of mission command.

Qualitative research method was used to understand the perception of mission command among the students of JCGSC. Semi-structured interviews were conducted with fifteen students. Students were chosen randomly, not in line with any specific service branch. Participants are skilled officers (eleven majors and four lieutenant colonels) with no less than ten years of experience as officers. Most have had leading positions in the units, from platoon to company size or branch-head positions in the staff. The interviews lasted for thirty to forty-five minutes, and the participants were asked questions from a standardised interview guide (Annex 1). This approach enabled the researcher to collect specific data and, at the same time, maintain the structure of the study. This research method ensures that the military cultures and professional experiences of the participants were well captured to enrich the findings. The qualitative research method and interviews provide a strong basis for identifying similarities and differences between the students, which serves as the foundation for analysis.

A systematic approach has been adopted to the current research for data collection and preparation to enhance the reliability and objectivity of the findings. Interviews were conducted using open-ended questions to obtain complete answers regarding theoretical knowledge, practical experiences, perceptions and challenges associated with mission command. Participant identifiers were anonymised to ensure confidentiality, and recordings were transcribed into WORD files. This approach ensured that the data collected were the real perceptions of the participants and, at the same time, left a good trail for the analysis of the themes. The application of an interview matrix also helped in arranging the data in a better and more coherent manner. The methods mentioned above helped build a strong base for analysing the perception of JCGSC students and drawing appropriate conclusions.

The interview guide provides a comprehensive framework to gather nuanced insights into the perception of JSGSC students on mission command. It was structured to elicit data across several areas. The guide starts with worm-up questions, which allowed to collect information about participants military background, familiarity and experience with mission command. The second part of the questions was designed to collect theoretical viewpoints by exploring how officers define mission command, its fundamental principles and the perceived alignment between theoretical training and real-world applications. The third part, practical experience questions, aims to determine how officers have observed or applied mission command principles and what issues they encountered. It also explores how experience complements or contradicts theoretical knowledge. In the fourth part of the questions, the guide dives into subjective perception by examining how mission command enhances trust, the levels of initiative, and whether such a concept is perceived differently with different experience levels in the field. It seeks to obtain comparative insights to evaluate differences in understanding and implementation depending on the experience level. The fifth part, the challenges and suggestions, gathers practical advice on limitations to implementing mission command and how military education and training can be adjusted to improve its adoption. By asking participants to reflect on barriers and propose improvements, the guide attempts to identify systematic issues and opportunities for enhancement. Overall, the interview guide is designed to ensure that the understanding of the mission command is integrative and pragmatic by combining theoretical and practical perspectives with personal experiences and more general considerations regarding military education.

In the analysis part, the interviews will be analysed based on the explanation provided for the interview guide, incorporating the theoretical findings from chapters one and two. Presenting the reader with the analysis results and leading to the conclusions and recommendations for continued academic improvements.

Results

In this chapter, qualitative data collected from the fifteen participants of the JCGSC will be discussed to understand the students' perceptions of mission command. After data analysis, insights were divided into three comparative groups: three Baltic state (3B)

NATO officers, other NATO officers and non-NATO officers. Similar ideas of the students will be combined, and at the end of the sentence, in brackets, the interviews in which it was found will be shown. The findings were analysed through five parameters: military background and familiarity, theoretical viewpoints, practical experiences, trust and initiative, and challenges with suggestions.

Military experience shapes familiarity with mission command, with varying levels of expertise observed among 3B NATO, other NATO, and non-NATO officers. All interviewed students reported that they are familiar with the mission command concept, however some of non-NATO country students heard about this concept for the first time in JCGSC during the leadership module. 3B NATO and other NATO officers reported an efficient and systematic encounter with mission command principles throughout PME (I02, I13, I06, I15, I12, I01). Nevertheless, 3B county interviewees described a hybrid experience, balancing Soviet legacies with NATO doctrines (I03, I09). Non-NATO officers noted late-stage exposure through NATO-led programs (I14, I05). This breakdown highlights clear differences between the three groups. Other NATO officers benefit from early and structured exposure, fostering familiarity with mission command. 3B NATO officers operate in a transitional space, balancing NATO integration with the remnants of their Soviet military heritage. Non-NATO officers face a steep learning curve, with their familiarity largely shaped by external influences from NATO. Students' different military backgrounds provide a foundational context for exploring how each group understands and applies mission command, which will be discussed in the following paragraphs.

Other NATO officers have a broader theoretical understanding of mission command than non-NATO or 3B NATO officers, yet some students of other NATO countries encounter similar issues. Other NATO officers defined mission command as a philosophy built on trust, shared clear intent, disciplined initiative and acceptance of prudent risk (I02, I12, I01, I07, I06, I13, I15). That is reminiscent of the ideas of the US Army Doctrine ADP 6-0 and NATO Doctrine AJP-01 principles. However, officers from other NATO countries identified issues in regularly implementing mission command principles due to reliance on hierarchical command structures and the existence of specific regulations (I04, I11). 3B NATO officers shared theoretical understandings the same as other NATO counterparts but emphasised a need for more scenario-based training (I08, I09, I03). This coincides with the findings from chapter two and the necessity to incorporate operational-level examples into PME. Non-NATO officers described mission command as an ideal structure that is often impossible to implement due to structural constraints (higher command blocking initiative, using strict mission orders due to existing direct command leadership style) and a lack of practical experience (I14, I10, I05). Strong theoretical basis supporting mission command in leadership roles helps other NATO officers. However, even within other NATO, some officers encounter difficulties in fully shifting to decentralised command structures. Non-NATO and 3B NATO officers, conversing with the theoretical foundation, have practical challenges due to systemic impediments and insufficient hands-on training. These theoretical differences lay the basis for investigating how officers execute mission command principles in real-world operations.

Other NATO officers generally report consistent application of mission command, while non-NATO and 3B NATO officers face systemic and cultural barriers to its practical implementation. Students from other NATO countries provided practical examples of mission command during multinational operations, emphasising trust adaptability and decentralised leadership (I06, I01, I07, I04, I15, I13). 3B NATO officers expressed partial adoption of mission command in joint exercises but admitted reliance on direct command in routine operations (I09, I03). Non-NATO officers’ practical experiences with mission command were more limited because of inexperienced subordinates and cultural barriers or higher command which preferred to use directive command (I14, I05, I10). Other NATO officers' practical experience validates mission command's operational efficacy. However, 3B NATO and non-NATO officers highlight the difficulties of integrating decentralised leadership into rigid command structures. Practical challenges in applying mission command reveal the critical role of trust and initiative, explored next.

All students underlined trust and initiative as vital for decentralised execution; despite that, 3B NATO and non-NATO officers identified challenges in developing these qualities. The majority of students confirmed that more experienced officers find it easier to apply the principles of mission command; however, some students from other NATO countries noted that these qualities are equally essential regardless of an officer’s level of field experience (I13, I12). Students from other NATO countries emphasised regular feedback, mentorship, open communication and shared objectives as mechanisms for trust-end encouraging initiative (I12, I15, I01, I13, I06, I07). 3B NATO officers recognised high turnover rates and limited leadership experience among junior officers as a challenge to creating trust. Still, they stressed that both experienced and new people could benefit equally from mission command once trust and initiative were developed (I08, I09). Non-NATO students highlighted that trust was frequently conditional, formed by structural constraints and a fear of mistakes, which hampered initiative (I14, I10). Some officers underlined that effective implementation of mission command relied on the leadership environment and organisational culture rather than individual field experience levels (I12, I13). Trust and initiative are viewed as definitive components of mission command efficiency across all groups; besides that, non-NATO and 3B NATO officers encounter structural and cultural obstacles that prevent trust-building. Several officers have observed that field experience levels have no substantial impact on mission command performance. These trust-related problems have a direct influence on mission command effectiveness, as seen by the broader systemic limitations outlined below.

Systemic issues to mission command exist across all groupings, while the nature of these challenges differs. Other NATO officers observed that upper command frequently hesitates to distribute responsibility for fear of career consequences, resulting in too specific directions. Non-NATO officers shared this worry, describing a similar tendency among higher commanders to micromanage in fear of making mistakes, undermining trust and initiative (I06, I07, I04, I14). Additionally, other NATO students identified barriers as a lack of trust in subordinates and highlighted the need for training and mentorship to build trust and develop initiative (I12, I02). Operational complexity in multinational contexts was also reported, emphasising the challenges of aligning mission command principles across diverse teams (I01, I06). 3B NATO officers underlined the necessity for mentorship programs, PME changes and enhanced collaboration with NATO allies to improve leadership competencies. In contrast, one officer recognised the importance of changing from centralised control to decentralised execution (I09, I03, I08). Non-NATO officers encountered additional systemic obstacles, such as outdated command structures, insufficient training resources, and unprofessional personnel. They suggested educating higher-level commanders on mission command principles to guarantee consistency across the chain of command and early inclusion of mission command principles into PME to ease cultural adaptation (I05, I14, I10). Higher leadership's unwillingness to hand over responsibility, as witnessed by both other NATO and non-NATO officers, represents a more significant cultural difficulty that undermines mission command principles. This issue highlights the importance of leadership training that promotes trust, accountability, and decentralised decision-making. Non-NATO and 3B NARO officers, who face additional systemic impediments such as outdated structures and resource deficits, need reforms and specific mentorship programs to address these problems. Addressing these challenges through tailored training and structural reforms is essential for fostering mission command across all groups.

This analysis reveals notable differences in how mission command is perceived and implemented among 3B NATO, other NATO, and non-NATO officers. Focusing on reforming PME, leadership training, and operational exercises are necessary to close these gaps, especially for higher commanders who have not been familiarised with these instruments during their military training. Military organisations can enhance mission command in diverse operational settings by building trust, promoting initiative, and connecting theoretical knowledge with real-world applications.

Conclusions

The JCGSC student's understanding of mission command is shaped by their acquired theoretical knowledge and practical experiences in their military career. A qualitative approach was used to analyse students' perceptions, and semi-structured interviews were conducted with Baltic Defence College JCGSC students. The data was categorised into three groups: 3B NATO, other NATO, and non-NATO nations. This methodology caught a variety of perspectives on mission command, influenced by military background, academic understanding, and operational experience.

The comparison research revealed considerable differences in the perception and application of mission command principles. Despite this, almost all students were familiar with the concept of mission command. Other NATO officers displayed a better understanding of decentralised command, identifying trust and initiative as critical components of its effectiveness. 3B NATO officers demonstrated a mixed knowledge shaped by Soviet-era hierarchy and NATO integration. Non-NATO officers noted structural and cultural barriers, including outmoded command methods and a lack of trust. Regardless of their differences, all groups underlined the importance of mentorship, training, and organisational reforms in overcoming challenges to mission command implementation.

PME is essential to embedding mission command in the military culture as a critical thinking, fostered by an appropriate curriculum, helps military leaders understand higher command intent and act creatively in operations. Leaders must first grasp the concept of mission command, as a lack of a theoretical foundation leads to inconsistent and superficial practice. According to Vandergriff and Murray, current training methods frequently rely on rote learning, which hinders the development of initiative and adaptability; students with limited operational experience struggle to bridge the gap between theory and practice, emphasising the importance of mentorship and experiential learning through actual settings. The philosophy of mission command is fundamentally based on the Prussian principle of *Auftragstaktik*, as a modern leadership philosophy that aims to ensure decentralised decision-making and operational flexibility, allowing commanders to delegate responsibility to subordinates while maintaining a clear commander intent and strategic purpose. As doctrinal literature emphasises, successful mission command is based on mutual trust, clear formulation of objectives, and the ability to respond to dynamically changing conditions. This was also stressed by the interviewees.

Recommendations

Based on the research findings, specific recommendations are essential to tackle the obstacles of integrating mission command principles into military leadership.

1. Scenario-based training during leadership model. To reduce the gap between theoretical and practical knowledge and implementation of mission command, including historical battles analysis and real-world scenarios that reflect the complexity of modern warfare.
2. Critical thinking integration. Incorporate critical thinking activities into the course to push leaders with challenging problem-solving responsibilities, promoting innovation and flexibility vital for mission command.

3. Decentralised command structures and trust-building initiatives**.** Conduct workshops to promote trust and initiative at all command levels, reinforcing decentralised decision-making, recommending reforms to reduce micromanagement and empower subordinate decision-making.

4. Promote mentorship programs. Establish mentorship initiatives pairing field experienced officers with less experienced ones to bridge gaps in practical understanding.

5. Update leadership assessments: Implement feedback systems that reward autonomy and adaptability, reducing fear of failure among commanders.

Bibliography

ADP 6-0. **Department of the Army, 2012.** Mission Command. ADP 6-0. Washington, DC: Headquarters, Department of the Army. [Online] 17 MAY 2012. [Cited: 5 NOV 2024]. Available at: https://www.moore.army.mil/mssp/security%20topics/Global%20and%20Regional%20Security/content/pdf/adp6_0_new.pdf.

AJP-01. **NATO standardisation office, 2022**. AJP-01: Allied Joint Doctrine. Edition F, Version 1. Brussels: NATO Standardization Office, December 2022, p. 85-87. [Online] 19 DEC 2022. [Cited: 8 NOV 2024]. Available at: https://www.cimic-coe.org/resources/external-publications/ajp-01-edf-v1-f.pdf

Ben-Shalom, Uzi and Shamir, Eitan, 2011. Mission command between theory and practice: the case of the IDF. *Defense and Security Analysis*. Vol. 27, no. 2, p. 101–117. [Online] 15 JUN 2011. [Cited: 23 OCT 2024].

Boyd, John, 2007. Patterns of conflict. [Online] 27 FEB 2005. [Cited: 7 NOV 2024]. Available at: http://www.projectwhitehorse.com/pdfs/boyd/patterns%20of%20conflict.pdf

Freund, Lucas, 2019. Transformational Leadership and Ethical Values. [Online] FEB 2019. [Cited: 12 DEC 2024]. Available at: https://www.researchgate.net/publication/330997524_TRANSFORMATIONAL_LEADERSHIP_ETHICAL_VALUES

Givens, Roger J., 2008. Transformational leadership: the impact on organisational and personal outcomes. School of Global Leadership & Entrepreneurship, Regent University. [Online] 2008. [Cited: 12 JAN 2025]. Available at: https://www.regent.edu/wp-content/uploads/2020/12/ELJ_V1Is1_Givens.pdf

King, Anthony C., 2017. Mission Command 2.0: From an individualist to a collective model. The US Army War College Quarterly Parameters. Vol. 47, no. 1. [Online] 1 March 2017. [Online] 15 JUN 2011. [Cited: 25 OCT 2024]. Available at: https://press.armywarcollege.edu/cgi/viewcontent.cgi?article=2832&context=parameters

Murray, Nicholas, 2014. The Role of Professional Military Education in Mission Command. Joint Force Quarterly, Issue 72, 1st Quarter. Washington, DC: National Defense University Press. [Online] 2014. [Cited: 28 SEP 2024]. Available at: https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-72/jfq-72_10-13_Murray.pdf

Nilsson, Niklas, 2021. Mission command in a modern military context. *Journal on Baltic Security*. Vol. 7, no. 1, p. 5–15. [Online] 13 May 2021. [Cited: 4 OCT 2024]. Available at: https://doi.org//10.2478/jobs-2021-0001

Nissinen, Vesa, 2001. Military Leadership: A Critical Constructivist Approach to Conceptualizing, Modeling, and Measuring Military Leadership in the Finnish Defence Forces. [Online] 30 NOV 2001. [Cited: 4 OCT 2024]. Available at: https://www.doria.fi/bitstream/handle/10024/125761/Military+Leadership-web.pdf?sequence=2

Ploumis, Michail, 2020. Mission command and philosophy for the 21st century. Comparative Strategy. Vol. 39, no. 2, p. 209–218. [Online]. 3 March 2020. [Cited: 4 OCT 2024]. Available at: https://doi.org/10.1080/01495933.2020.1718995

Shamir, Eitan. 2011. Transforming Command: The Pursuit of Mission Command in the U.S., British, and Israeli Armies. Stanford, CA: Stanford University Press. [Online] 2011. [Cited: 12 DEC 2024]. Available at: https://books.google.ee/books?hl=en&lr=&id=3-1WLAB7spUC&oi=fnd&pg=PR7&dq=Shamir,+2011+mission+command&ots=TQUcjlArDn&sig=ehsxUM1uzmL7zYTnK-KjhVOSmz4&redir_esc=y#v=onepage&q=Shamir%2C%202011%20mission%20command&f=false

Siuparis, Alvydas. 2024. Introduction. *Baltic Military History Conference:* Professional Military Education in the Baltic Region 1919-2024, Tartu, 31 OCT 2024

Sonnenberger, Martin and Art of War Scholars, 2013. Initiative within the Philosophy of Auftragstaktik, Determining Factors of the Understanding of Initiative in the German Army 1806-1955. Master's Thesis. US Army Command and General Staff College. [Online] 2013. [Cited: 20 SEP 2024]. Available at: https://apps.dtic.mil/sti/pdfs/ADA599111.pdf

Vandergriff, E. Donald, 2019. *Adopting mission command, developing leaders for a superior command culture*, p. 54-67, 101-196. Annapolis, Maryland: *Naval institute press,* 2019.

Wong, Leonard, Bliese, Paul, and McGurk, Dennis, 2003. Military Leadership: A Context Specific Review. Washington, DC: Walter Reed Army Institute of Research. [Online] DEC 2003. [Cited: 19 DEC 2024]. Available at: https://www.sciencedirect.com/science/article/pii/S1048984303000559

List of annexes not published, known to publisher and author and can be requested via info@baltdefcol.org.
Annex 1. Interview Guide: JCGSC Students' Perceptions of Mission Command
Interviews:
Annex 2. I01
Annex 3. I02
Annex 4. I03
Annex 5. I04
Annex 6. I05
Annex 7. I06
Annex 8. I07
Annex 9. I08
Annex 10. I09
Annex 11. I10
Annex 12. I11
Annex 13. I12
Annex 14. I13
Annex 15. I14
Annex 16.

MAJ Veiko Dieves Wargaming as a capability development tool

Introduction

Wargames are in the military context mostly used for studying tactical, operational and strategic problems (Teppo, 2019, p. 30). Wargaming is suitable for investigating complex and dynamic processes because it is itself dynamic and complex (Hanley, 1991, p. 13). Wargaming is considered to be a cost-effective method for studying complex and intricate problems (Dunnigan, 2000, pp. 317–324). According to McGrady and Perla, wargaming is the simulation of warfare, where the participants' decisions influence the final outcome (Perla, McGrady, 2007). It has been argued that wargaming is suitable for studying combat operations as a process involving friction and uncertainty (Teppo, 2019, p. 30).

Other than simulating outcomes in complex tactics, wargames can also be used for capability development, for testing and validating new concepts and technologies. Before deploying new systems or operational approaches in real-world operations, military organisations can use wargames to evaluate their effectiveness and identify potential weaknesses. For example, the Estonian Defense Forces (EDF) are deciding between different capability command and control (C2) options for its artillery units. As the problem itself is complex, wargaming as a method is used to evaluate different capability options. This research paper aims to develop a wargaming method suitable for that purpose: comparing and assessing different C2 options for military capability. Given the evolving security challenges in Europe and advancements in technology, Estonia (Estonian Ministry of Defence, 2020) and European nations (European Commission, 2025, pp. 1–4) are likely to develop numerous additional military capabilities over the next decade. To ensure effectiveness, adopting a scientific approach to capability development is crucial, with specialized wargaming methods serving as a strong foundation for this approach.

For that purpose, the author created the following research questions:

1) What are the main design principles of wargames used for capability development?
2) What were the outcomes of EDF wargame experiment?
3) How should the wargame design principles be improved?

The research paper is divided into three parts. First, the author gives an overview of wargame design principles used to conduct capability comparisons. Second, the author describes the experimental wargame conducted in EDF for the very purpose of capability development. In the third part, the research paper discusses the experiment's findings, compares the wargame with theoretical approaches, and discusses what approach worked well during the experiment and where improvements should be made. The author offers, in the conclusion part, recommendations for future wargames.

1. Wargaming as a method for capability development

This chapter gives an overview of the wargaming theory and describes the main principles of wargame systems used to conduct capability comparisons.

NATO Supreme Allied Commander Transformation (SACT) and Bundeswehr define wargaming as “a method that uses scenario-based models to represent conflict or competition in a safe-to-fail environment, in which events, human decisions and resulting outcomes mutually influence one another” (*Bundeswehr Wargaming Handbook*, 2024, p. 14).

Wargames are typically divided into learning games and analytical games (SACT, 2023, p. 5). While learning games are used to train units and individuals in their decision-making skills, analytical games are used to answer research questions through exploration of a problem in greater detail, testing a hypothesis or assessing solutions (SACT, 2023, p. 12).

Analytical wargames have to be designed around the research questions. Wargame analysis has to be taken into account during the design and development process of analytical wargame. This process has to accommodate the lead analyst from the beginning. Key elements for analysis include problem formulation, selection of appropriate methods, selection of wargame aim and objectives, bias check and adjudication.(SACT, 2023, p. 22)

NATO Supreme Allied Commander Transformation views general wargame design process as follows:

1) Initial event preparations – this step includes logistical and organizational aspects of running the wargame;
2) Data collection and analysis plan creation - this step includes a description of data collection methods, measures, and research questions;
3) Rules and mechanics creation – this step addresses player goals, number and length of turns (time-system in use), player inputs and adjudication method.(SACT, 2023, pp. 25–28)

Bundeswehr's wargaming methodology defines wargaming through added complexity. When researching a question, a corresponding model is created. If that model is examined over a period of time, those models become simulations. If at least two parties characterized by human behaviour interact in the simulation, this simulation becomes a simulation game. If a simulation game involves a conflict situation, this becomes a wargame. (*Bundeswehr Wargaming Handbook*, 2024, p. 8)

Bundeswehr builds on top of the NATO wargaming model, adding to the analytical and educational axis additional parameters. Wargaming is separated into 3 levels: tactical, operational and strategic. In addition to that, the scope of the wargaming spans from tactical to strategic and from the past to the future. (*Bundeswehr Wargaming Handbook*, 2024, p. 9) Bundeswehr wargaming scope is depicted in figure 1.

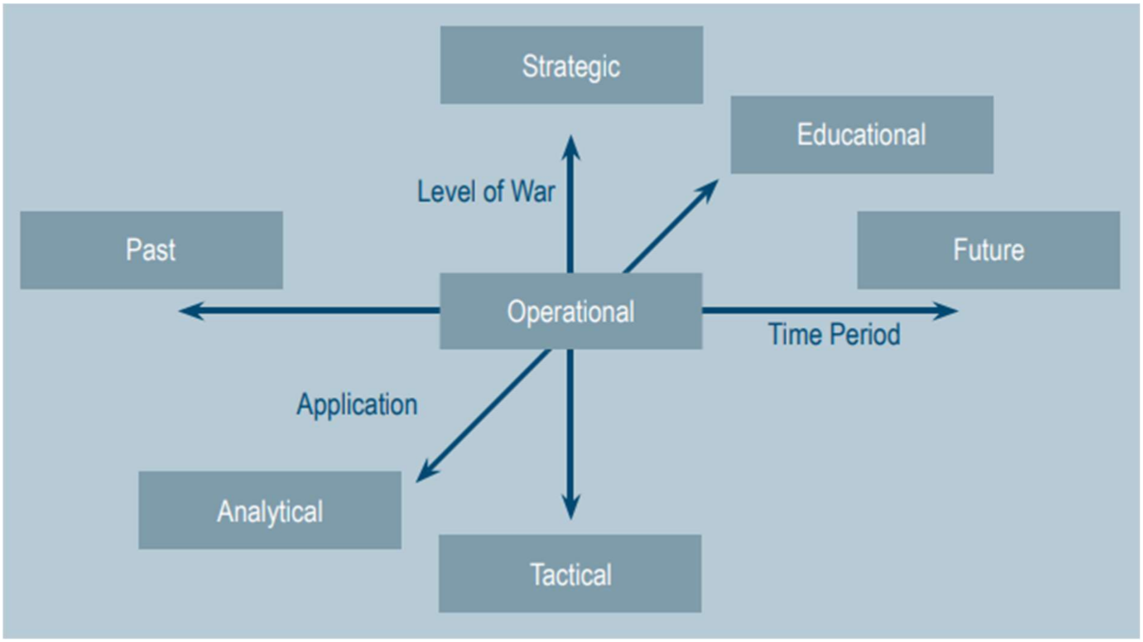

Figure 1. The scope of wargaming. Source: (*Bundeswehr Wargaming Handbook*, 2024, p. 9)

Bundeswehr sees the purpose of analytical wargames as to answer specific questions and to find solutions in complex and uncertain situations (*Bundeswehr Wargaming Handbook*, 2024, p. 12). Wargaming has to provide qualitative correlation indicators that help understand specific processes and questions better (*Bundeswehr Wargaming Handbook*, 2024, p. 13). Bundeswehr uses analytical wargaming for concept development, experimentation, and operations research (*Bundeswehr Wargaming Handbook*, 2024, p. 14).

United Kingdom (UK) Ministry of Defence Wargaming Handbook defines wargaming through decision-maker immersion and problem complexity. Wargaming is seen as a decision-making technique that helps explore relatively low-cost approaches that work and what does not work. Wargaming is a simulation of selected aspects of a conflict, using predetermined rules, data and procedures to provide decision-making information and experience for real-world situations.(*Wargaming Handbook* 2017, pp. 5–6,10)

Previously, wargaming has been used for capability development in the UK to develop their Light Battlegroup concept. The described approach begins with comprehensive background research and analysis, including a SWOT (Strengths, Weaknesses, Opportunities, and Threats) assessment and leveraging broader military judgment to frame the operational context. This is followed by modelling force comparisons and conducting mobility analyses. A unit-level MAPEX (Map Exercise) wargame then examines specific tactical considerations. Industry engagement further informs the process, culminating in a final MAPEX wargame to validate and integrate findings.(England 2015)

UK's Light Battlegroup concept development approach is depicted in figure 2.

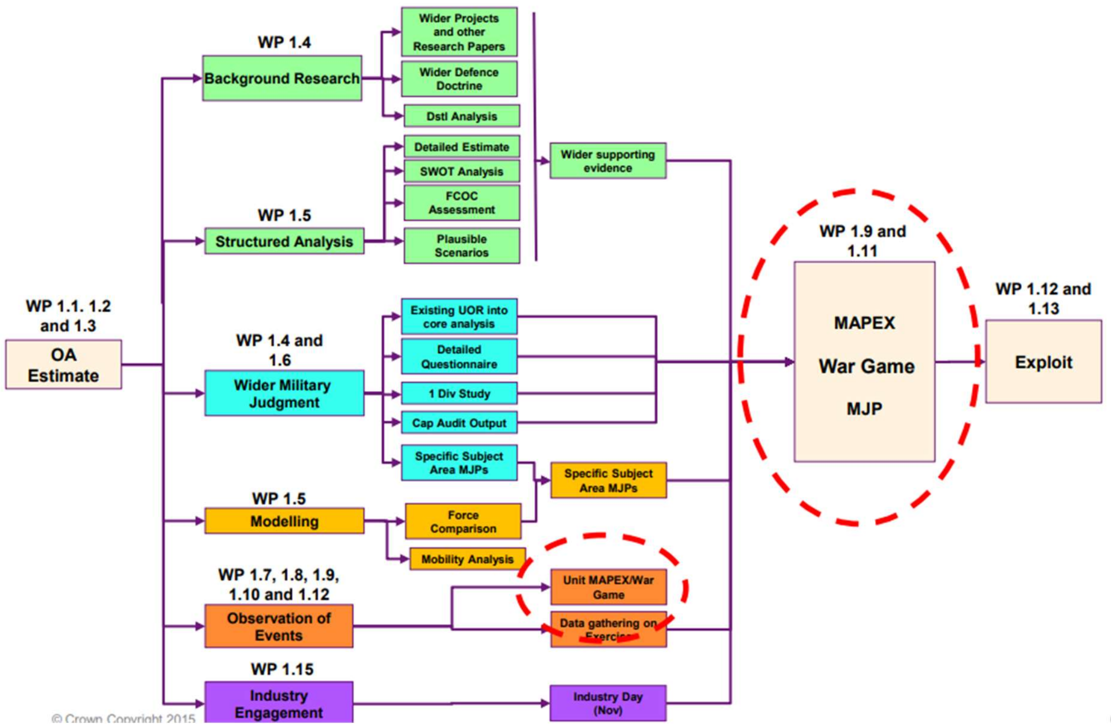

Figure 2. UK's Light Battlegroup development approach. Source: (David England, 2015, p. 6)

UK's Defence Science and Technology Laboratory conducts regular analysis of the force testing process to shape the structure and tasks of the UK Armed Forces. Those analyses are used for capability planning, equipment programmes and unit structures. Military response options are identified in the strategic planning phase and moved to the campaign planning phase. Here, courses of action are developed and tested with some wargaming. Initial analysis and testing happen during this phase, but not a full wargame. Depending on the results, all or some courses of action move to the execution phase for detailed testing. The main result of the planned force testing execution wargames is a narrative detailing the campaign's progression. This includes vignettes for specific activities, player insights, and the overarching risks and issues from the campaign. The narrative forms the basis for further detailed analysis, leading to various reports and recommendations.(*Wargaming Handbook*, 2017, pp. 70–72).

The United States Army War College Wargame Handbook outlines that the foundation of effective wargame design begins with a clear definition of purpose, scope, and objectives. Designers must articulate the specific questions the game intends to answer – whether for analytical insight, training, or strategic planning. This involves establishing precise parameters such as the key variables to be simulated, roles for participants, and the decision-making processes that mirror real-world complexities. The goal is to construct a simulation that reflects the operational environment without becoming overly intricate, balancing realism with manageability. (*Strategic Wargaming Series Handbook*, 2015, pp. 9–10)

Equally important is the structured, iterative design process that The United States Army War College Wargame Handbook advocates. This process is divided into four phases: planning, preparation, execution, and debriefing. During the planning and preparation stages, designers select appropriate rules and mechanisms to ensure the game engages participants and serves its analytical purpose. The execution phase tests these decisions in a controlled simulation where dynamic challenges emerge. Finally, a comprehensive after-action review captures lessons learned, informing future game iterations. This cyclic methodology not only refines the design of individual wargames but also contributes to the broader understanding of military decision-making and strategic thinking. (*Strategic Wargaming Series Handbook*, 2015, pp. 3–4).

While wargaming offers significant benefits in strategic planning and decision-making, it is important to acknowledge its drawbacks. One notable limitation is that wargames are time- and resource-intensive, often requiring substantial investment in personnel, time, and financial resources. This can make them less accessible for routine strategy development, leading organizations to reserve wargaming for addressing extraordinary challenges rather than as a standard tool. Consequently, the effectiveness of wargaming is contingent upon decision-makers' willingness to allocate the necessary resources and their conviction in the added value of this method (Werro, Nitzl, Borghoff, 2024).

Wargames have been widely applied in real-world military settings to support capability development by enabling structured comparisons of different force options, technologies, and operational concepts. The following examples illustrate how wargaming is used to guide capability decisions:
RAND Corporation conducted a series of tabletop wargames to assess NATO’s ability to defend the Baltic states against a potential Russian incursion. These games highlighted severe capability gaps in forward-deployed forces and led to recommendations on strengthening NATO posture, enhancing mobility, and investing in precision fires. (Shlapak, Johnson, 2016, pp. 1–2).

In the U.S. Army's annual wargame, senior leaders use strategic simulations to assess and prioritize infrastructure funding decisions. These wargames serve as a platform to evaluate scenarios, identify potential challenges, and determine the most effective allocation of resources to enhance the Army's operational readiness and infrastructure resilience. The US Army can develop and refine capabilities through wargames, ensuring infrastructure investments align with strategic objectives (Alford, 2023).

The U.S. Marine Corps uses wargaming to assess and develop operational and strategic planning capabilities. Through structured simulations and scenario-based exercises, wargames enable the evaluation of current capabilities and identifying future requirements. This approach supports informed decision-making and enhances readiness by testing strategies in dynamic and complex environments. (Maurer, 2019)
NATO STO SAS-151 working group has developed a prototype multi-layer wargame to support the development of the intermediate force capability concept by bridging tactical and strategic dimensions. This approach enables warfare simulation across multiple scales, ensuring a balance between capturing complexity and avoiding oversimplification. The wargame provides a structured framework to evaluate capabilities, test strategies, and inform decision-making processes (Dobias, Nelson, 2023, pp. 33–1).

In conclusion, the wargames used in capability development are purpose-built analytical tools. These games must begin with clearly defined research questions and objectives guiding every design aspect. This ensures that the wargame focuses on exploring specific capability challenges and produces insights that directly inform development decisions.

The design process is iterative, moving through planning, preparation, execution, and evaluation. Each iteration refines the game's structure and scenario to address the research aims. Feedback from previous runs is essential for improving game fidelity and analytical value.

A careful balance between realism and simplicity is essential. The wargame must realistically reflect the operational environment yet avoid unnecessary complexity that could obscure key dynamics. The focus should remain on clarity, usability, and generating meaningful comparisons between options.

Human decision-making is central to the design. Wargames must simulate actual roles, pressures, and choices so that participants interact and respond in ways that mirror real-world operations. This interaction reveals the strengths and limitations of different capabilities.

The scope and scale of the game must match the level of analysis – whether tactical, operational, or strategic – and focus on a timeframe and context appropriate to the capability in question. A well-defined scope prevents drift and ensures relevant findings.

Incorporating real-world tools and systems, such as command-and-control platforms or logistics data, enhances realism and allows players to engage with the game environment in familiar ways. This improves both immersion and the reliability of results.

Scenario development has an important role in the process. A well-framed scenario sets the stage for meaningful decisions and tests, embedding the game in a plausible and operationally relevant narrative. Event scripting should support immersion and drive purposeful gameplay.

Finally, robust data collection and post-game analysis are essential. Predefined metrics must be tracked to assess performance, and structured debriefs must interpret results. This allows insights from the game to feed directly into capability development decisions.

Together, these principles form a comprehensive approach to designing wargames that support military capability development.

2. An experiment in the Estonian Defence Forces

During the last 3 years, EDF has gone through significant reforms, most notably creating the Estonian 1st Division (Vabariigi Valitsus, 2022). Part of creating a division has also been creating new fire support capabilities that can enable divisional battle. Creating the new capabilities has initiated the EDF's endeavour to identify a C2 structure optimized for integrating and utilising new operational assets. The decision to conduct the wargame provided a structured framework for assessing the strengths and weaknesses of these capability variants, allowing for informed discussions and evaluations that ultimately shape the development of future capabilities.

30SEP24, a wargame was conducted in the Estonian Division HQ to form a basis for selecting a capability variant for the Estonian Artillery Force. The wargame was the basis for tactical discussion that took place after the game in the form of AAR[1] and was itself an input in deciding the capability development variant. Because the info about the selected capability variant is for official use only, this research paper does not discuss the capability variant or the exact game scenario and specific numerical results of the game but generalizes the process to draw relevant conclusions.

[1] AAR – After Action Review.

To start the wargame design process, the wargame organizing team[2] led by this research paper's author started with engaging stakeholders from the Estonian Division and artillery community to ensure that the wargame's purpose was agreed upon and aligned amongst the main stakeholders. Following the purpose alignment, the problem statement was proposed and validated with key personnel to design the wargame. After the problem statement, research questions were formulated. Those research questions were then validated with a discussion among subject matter experts. To answer these questions, the wargame design team selected relevant measurable parameters. After the parameters selection step, the design team selected agents and actors in the game who could produce the information that could be measured to answer the research questions. Then, capability variants were mapped using the network diagram method, where relevant agents and actors were described by stating their connections to other actors and services/tasks that those actors carry out (Fig 3).

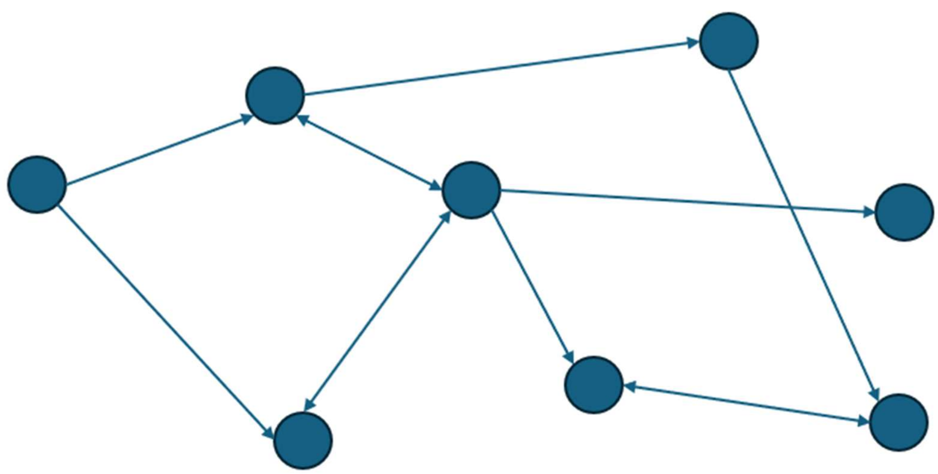

Figure 3. Example capability variant network diagram, simplified.

Actors network diagrams were the basis for defining the game structure. The game structure consisted of actors and external roles that were only needed to provide input information to actors and to receive output information from game actors. It is important to define inputs and outputs so that participants interact with other actors in a way that mimics the closest the real interactions they would have in the real world. This enables the participants to make decisions, interact, and take actions that closely mirror real-

[2] Team had two members, the author and mr Markus Veinla, MSc.

world operations, minimizing the influence of artificial constraints imposed by the game design. This approach ensures the wargame generates authentic insights, with outcomes validated by participants and the clientele.

In the next step, the author designed the Main Event List/ Main Incident List[3] for the wargame, defined the input and output format, and created other operational products like KOLT[4] and Tooru[5] virtual operations. As both KOLT and Tooru are the primary systems used for battle management and fire support within the EDF, their inclusion in the wargame design enhanced realism for the participants.

Two sequential scenarios were conducted during the game, each focusing on a different capability variant. MEL-MIL incidents were pre-scripted and initiated by two designated players, one of whom was the author. To highlight potential functional shortcomings, the sequence and details of the incidents were deliberately varied while remaining within the boundaries of the predefined MEL-MIL framework. The primary objective of these incident simulations was to activate and assess procedures and communication protocols within the adopted C2 structure, allowing participants to engage in realistic decision-making and coordination processes.

Following the game, participants and divisional leadership engaged in a comprehensive discussion to evaluate the advantages and disadvantages of the two capability variants. This discussion shaped the understanding of the preferred capability variant, ultimately forming the foundation for the decision-making process. Thus, the wargame was an essential platform for informed deliberation and decision-making.

After the wargame, relevant information from the KOLT chats and Tooru fire mission logs were collected and analysed to assess the decision-making efficiency and information management speed across the different capability variants. Specifically, the analysis of chats and logs focused on evaluating the average process speed, the

---

[3] The Main Event List (MEL) and Main Incident List (MIL) are structured tools used in wargame planning. The MEL outlines key events that drive the scenario forward, while the MIL specifies incidents or injects designed to prompt participant decisions and actions during the wargame.
[4] KOLT – EDF Battle Management System.
[5] Tooru – EDF Fire Support System.

percentage of fire missions utilizing appropriate assets, the percentage of timely engagement decisions, and the percentage of coordinated fire missions that were successfully executed. These metrics provided insights that contributed to the comprehensive evaluation and selection of the most suitable capability variant.

Finally, the author conducted a phenomenological study to gather participant feedback on the wargame system, utilizing their insights to refine and enhance the design of future wargames. A phenomenological study is a type of research focused on human experience (Laherand, 2008, p. 87). The outcome of a phenomenological study is the formulation of general conclusions about the subject being studied. Such a study is typically carried out in five stages. In the first stage, the researcher familiarizes themselves with the data set to gain a general overview (Laherand, 2008, p. 89). In the second stage, the data is broken down into meaning units that express significant aspects of the phenomenon under investigation. The third stage involves translating the interviewees' language into scientific terminology for a more structured material analysis. The fourth stage of phenomenological analysis consists of constructing individual meaning networks. A general meaning network is created in the fifth stage, addressing the phenomenon at a broader level. (Laherand, 2008, pp. 91–92)

The phenomenological aspect of this research involved conducting surveys among the primary (altogether 10) participants following the wargame. The author utilized ChatGPT 4o's Deep Research mode to analyse the collected responses to perform a comprehensive phenomenological study. The author then reviewed the AI-generated summaries of participant feedback, ensuring that the synthesized results accurately reflected the participants' original responses and were relevant and credible. The author also verified that the AI did not produce hallucinated information or premature conclusions based on isolated or particularly strong statements. This cross-checking process ensured that diverse perspectives provided by the participants were adequately represented, and any bias introduced by the AI due to contextual misunderstanding was mitigated to maintain the integrity of the analysis. Through this combined human-AI approach, the research findings were refined and validated, enhancing the overall reliability of the study. For that purpose, after the game, participants answered the following questions:

1) What are the most important parameters that a wargame measures/should measure?

2) What important parameters, in your opinion, did the game not measure/does not measure?

3) How reliable do you consider the results of the wargame?

4) What would you change in the structure and/or execution of the wargame (1 and/or 2) to better achieve the objective of the wargame (comparing the effectiveness of two capability solutions)?

5) What parts of the wargame's structure and/or execution do you not consider necessary to change to achieve the objectives? What works/worked?

The overall wargame research process is depicted in Figure 4. In summary, the method developed by the author comprises the following steps: wargame contextualization, stakeholder engagement and problem definition, formulation and validation of research questions, wargame design, game structure development, preparation of game tools, wargame playthrough, and post-game discussion and capability variant decision shaping. The decision-shaping process is further influenced by quantitative data analysis, which is used to compare different capability variants. Additionally, the phenomenological study contributes to the refinement of future wargame designs, aiding in developing wargaming methods tailored for capability development.

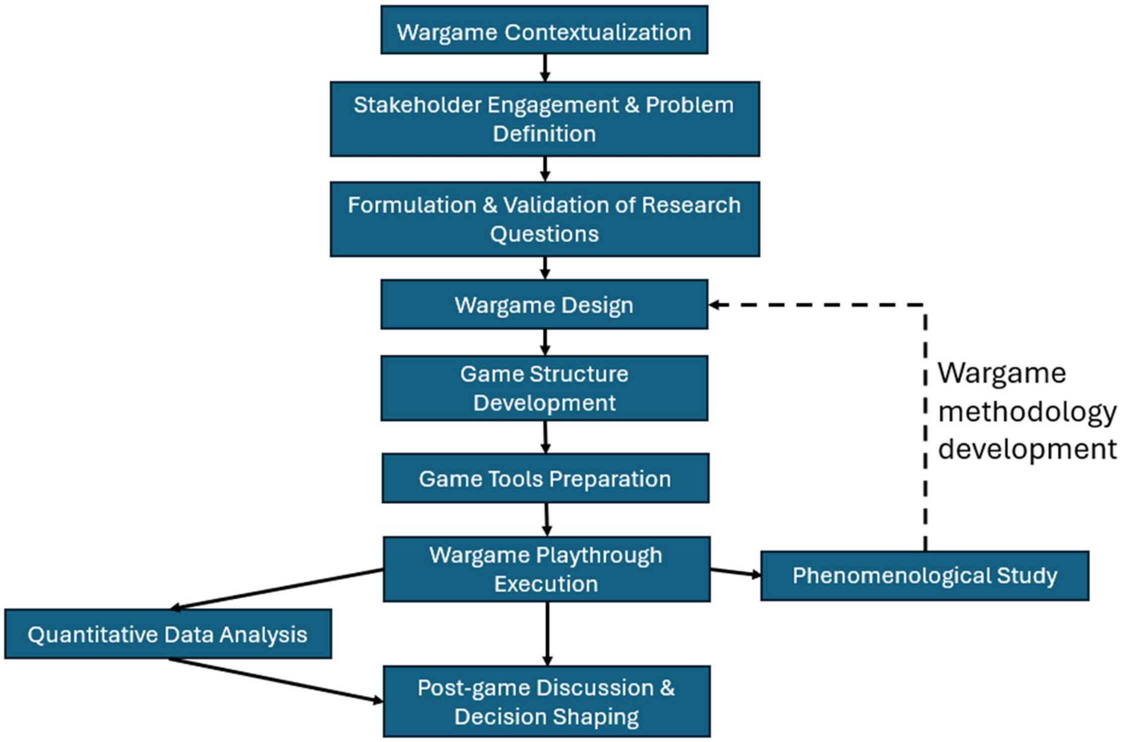

Figure 4. Wargame research process flowchart.

3. Insights from the Phenomenological Study

This chapter compares the theoretical wargame design principles with the practical outcomes of the EDF experiment. It analyzes participant feedback to assess the tools' effectiveness, identifies areas where the design worked well, and highlights aspects that should be modified to support capability development better. Finally, the chapter concludes with recommendations for improving future wargames

To support this analysis, participant feedback from the EDF wargame was systematically reviewed and organized by key themes. Insights were drawn across five main areas: (1) important parameters the wargame measures (or should measure), (2) important parameters that were not measured, (3) the reliability of the wargame's results, (4) suggested changes to improve the wargame, and (5) aspects that were effective and require no change. The following sections discuss findings in each area, summarizing the feedback and providing recommendations based on these insights

Participants generally agreed that the wargame measured several critical operational parameters. Many pointed to how quickly command levels made decisions and executed responses – from detection to strike – as key indicators. This reflects a perception of the game as testing the tempo of command and control under pressure. Participants also emphasized mutual understanding, proper task sequencing, and smooth information flow as indicators of successful coordination. These experiential markers suggest that players valued how the game tested teamwork and communication efficiency. Several players focused on whether the plan was achievable with available resources. Issues such as logistic chain resilience and ammunition resupply were highlighted as important parameters that were either measured or expected to be assessed. Participants looked for the game to reveal vulnerabilities and decision points. Identifying risks and opportunities was seen as a natural outcome of playing through the scenario. While mentioned less frequently, adaptability under pressure was seen as an important aspect of command effectiveness and something the game should emphasize. Overall, participants experienced the wargame as most valuable when it tested practical, real-world dynamics – especially speed, coordination, and logistical feasibility.

Despite its strengths, participants felt the wargame left key dimensions unexplored. Many observed that critical elements like force protection, sustainment logistics, and rear-area coordination were not part of the game. The absence of these systems made the simulation feel incomplete and less representative of actual operations. Real-world communication challenges – such as radio network congestion and signal delays – were not represented. This lack of fidelity reduced realism and the perceived value of tested communications systems. Participants noted that features in the simulation system (e.g., fire mission processing, logistics tracking) were available but unused. As a result, the game failed to assess coordination tools that would be vital in real scenarios. Some noted that different organizational structures or plans were not distinct enough or weren't meaningfully tested. Participants expected a comparative evaluation but did not experience clear contrasts between tested concepts. Several responses indicated confusion about what, if anything, was being measured. A lack of clarity around objectives and metrics left participants unsure about the game's analytical purpose. These gaps reflect an experiential disconnect between the game's intent and execution. Participants wanted a more holistic simulation that included logistics and communications and clearly tested variations in capability.

Participants' views on the reliability of the wargame's results were mixed. Some participants believed the results were "moderately reliable," especially where game design was sound and roles well-manned. However, many emphasized that results were only valid if the correct elements were included and executed properly. Where roles were missing (e.g., intelligence staff, air coordination) or simulation tools underused, participants questioned whether any meaningful conclusions could be drawn. There was concern about deriving "false lessons" from an incomplete simulation. Several participants argued that the results could only be reliable if the simulation accurately represented command structures and processes. Without full representation of key functions, confidence in insights was limited. In short, while participants valued the learning process, they cautioned against using the results as a standalone basis for decision-making unless game fidelity and scope were improved.

Clear objectives and metrics are essential for the effectiveness of a wargame. Participants need to understand what the game is designed to test and how performance is evaluated. Without a clear purpose, the simulation risks becoming directionless, and participants may struggle to engage meaningfully with the scenario. Defining the analytical goals at the outset allows all game elements – from scenario injects to participant behaviour – to align with those aims. A focused objective also ensures that results can be interpreted within a consistent framework, increasing their credibility and usefulness for capability development.

Functional completeness within the wargame structure is crucial in maintaining realism and analytical value. When critical roles such as logistics, intelligence, or fires coordination are missing, the game fails to replicate the complexities of real-world operations. Participants can then not fully explore the interplay between different functions, and important challenges – such as sustaining operations or managing information flow – are left untested. A comprehensive setup ensures that all dimensions of the operation are represented, allowing the wargame to produce insights that reflect the actual demands of capability deployment and coordination across domains.

Digital tools within the simulation environment must be fully integrated into gameplay to provide meaningful insights. When participants do not utilize available systems – such as fire support modules, logistics tracking, or situational awareness platforms – the wargame fails to measure how these tools influence operational effectiveness. Proper training and familiarization are necessary so that users can confidently interact with the technology during play. Only by fully engaging with these systems can the wargame assess how well digital infrastructure supports decision-making and coordination, especially under time pressure and operational stress.

Focusing on the scenario design helps to maintain analytical clarity within the wargame. Overly complex or diffuse scenarios can dilute the learning objectives and make attributing outcomes to specific decisions or structural differences difficult. Participants may struggle to discern the implications of their choices when too many variables are in play. By streamlining the scenario and highlighting the contrasts between tested alternatives, designers can ensure that the game generates meaningful comparisons. A well-focused wargame creates conditions where the intended hypotheses are clearly tested, and participants' actions can be directly linked to outcomes.

Improving briefings and communication protocols before and during the wargame enhances player performance and analytical value. Confusion can undermine coordination and delay decision-making when roles, objectives, and procedures are unclear. Standardizing communications – such as consistent call signs and reference formats – ensures that participants know who they interact with and what is expected. Thorough preparation, including pre-game rehearsals, allows participants to begin the simulation with confidence and shared understanding. Clear communication and preparation reduce friction and help maintain the tempo and coherence of the game, enabling more reliable observations and outcomes.

Despite areas for improvement, participants highlighted aspects that worked well and should be preserved. The Master Events List and associated injects were seen as well-structured and relevant. Even where execution fell short, the scenario was praised as realistic and engaging. Some players noted strong and simplified leadership during the game helped keep it on track. Effective facilitation played an important role in maintaining flow and engagement. The decision to have command posts work independently (as they would in real-world operations) was appreciated. Participants viewed this setup as a strength that added realism without unnecessary complexity. Many participants felt the wargame format itself was valuable. Despite its flaws, they endorsed continued use and iteration of such exercises for concept development and testing.

Conclusions

This study was conducted to develop a wargame method suited for military capability development. Specifically, the proposed method was used to test C2 approaches of artillery units in the Estonian Defence Forces. For that, the wargame was designed around the principles derived from theoretical literature. After the wargame, the author conducted a phenomenological study to evaluate and improve the proposed method.
The main principles of capability development wargaming include defining clear research questions and objectives, using an iterative design process with testing and feedback, balancing realism with simplicity, simulating human decision-making, aligning scope with analysis level, integrating real-world tools, designing meaningful scenarios, and ensuring robust data collection with structured post-game analysis.

The outcomes of the EDF wargame experiment were assessed through participant feedback. Analysis showed that the wargame was seen as a partially effective tool for examining decision-making, coordination, and operational feasibility. Valuable insights emerged on parameters such as C2 speed and mutual understanding. However, gaps—like missing support functions and unclear objectives—limited participant engagement and confidence in the results.

Participants recommended clarifying objectives and metrics to improve wargame design for capability development, ensuring all critical roles and processes are represented, and fully integrating simulation tools through proper training. Scenario design should be streamlined to focus on key comparisons, and preparation should be improved via briefings, rehearsals, and clear communication protocols. Elements that worked well—realistic structure, strong scenarios, and effective facilitation—should be retained.

Ultimately, these recommendations reinforce established wargame design principles – alignment with research questions, inclusion of appropriate participants, balance of realism and focus – and show how these principles resonate with actual participant experiences. Wargames can provide insight into capability development decisions when designed and executed effectively. However, as this analysis shows, realizing that potential depends on preparation, inclusive design, and clear purpose.

Bibliography

ALFORD, Stefan. 2023. Army prioritizes infrastructure funding at annual wargame. *US Army*. [Online]. 2023. [Cited : 25 March 2025]. https://www.army.mil/article/270405/army_prioritizes_infrastructure_funding_at_annual_wargame

Bundeswehr Wargaming Handbook, 2024. [Online]. Doktrinzentrum der Bundeswehr. https://www.professionalwargaming.co.uk/Wargame_Handbuch_englisch_online.pdf

DAVID ENGLAND. 2015. Wargaming Best Practice. *Connection UK 2015*. [Online]. 2015. https://www.professionalwargaming.co.uk/2016England.pdf

DOBIAS, Peter and NELSON, John. 2023. *Multilayer Wargames: Lessons from Gaming Intermediate Force Capabilities* [Online]. https://wargaming.hoover.org/file/8822/content

DUNNIGAN, James F. 2000. *Wargames handbook: how to play and design commercial and professional wargames*. 3. ed. San Jose, Calif.: Writers Club Press. ISBN 978-0-595-15546-0.

ESTONIAN MINISTRY OF DEFENCE. 2020. National Defence Development Plan 2026. [Online]. 15 September 2020. [Cited : 26 March 2025]. https://kaitseministeerium.ee/riigikaitse2026/eng/

EUROPEAN COMMISSION. 2025. *White Paper for European Defence – Readiness 2030* [Online]. Brussels, Belgium: European Commission, Defence Industry and

Space. https://defence-industry-space.ec.europa.eu/document/download/30b50d2c-49aa-4250-9ca6-27a0347cf009_en?filename=White%20Paper.pdf

HANLEY, J. T. 1991. *On Wargaming*. University of Michigan.

LAHERAND, Meri-Liis. 2008. *Kvalitatiivne uurimisviis [Qualitative research method]*. Tallinn. ISBN 978-9949-15-655-9.

MAURER, John. 2019. USMC Wargaming Capability. [Online]. 24 January 2019. [Cited : 25 March 2025]. https://slideplayer.com/slide/15986249/

PERLA, Peter P and MCGRADY, Ed. 2007. Wargaming and Analysis: Presentation for MORS Special Meeting. [Online]. Alexandria, Virginia. 2007. https://www.cna.org/archive/CNA_Files/pdf/d0016966.a1.pdf

SACT. 2023. *NATO Wargaming Handbook*. [Online]. Oberammergau, Germany: Allied Command Transformation. https://www.professionalwargaming.co.uk/nato-wargaming-handbook.pdf

SHLAPAK, David A. and JOHNSON, Michael. 2016. *Reinforcing Deterrence on NATO's Eastern Flank: Wargaming the Defense of the Baltics*. Erscheinungsort nicht ermittelbar: RAND Corporation. Research report, RR-1253-A. ISBN 978-0-8330-9298-4.

Strategic Wargaming Series Handbook, 2015. [Online]. Wright Avenue, Carlisle, PA: United States Army War College. https://csl.armywarcollege.edu/DSE/StrategicWargamingDivision/publications/USAWC%20Wargame%20Handbook%201%20July%2015.pdf

TEPPO, Lauri. 2019. Sõjamäng uurimismeetodina [Wargames – A Viable Research Method?]. *Sõjateadlane*. 2019. Vol. 12, pp. 30.

VABARIIGI VALITSUS. 2022. Valitsus otsustas diviisi loomise [The government decided on the establishment of a division]. *Vabariigi Valitsus*. [Online]. 12 August 2022. [Cited : 25 March 2025]. https://www.valitsus.ee/uudised/valitsus-otsustas-diviisi-loomise#:~:text=Stenbocki%20maja%2C%208.%20detsember%202022%20-%20Valitsus%20muutis,kaitsev%C3%A4e%20struktuuri%C3%BCksusena%20diviis%20vastavalt%20NATO%20Madridi%20tippkohtumisel%20kokkulepitule.

Wargaming Handbook, 2017. . Swindon: The Development, Concepts and Doctrine Centre.

WERRO, Aline, NITZL, Christian and BORGHOFF, Uwe M. 2024. *On the Role of Intelligence and Business Wargaming in Developing Foresight*. [Online]. 2024. arXiv. [Cited : 27 March 2025].

MAJ Taavi Liias. Can mission command survive advanced technologies?

Introduction

Technological developments in recent decades have been revolutionary. The military industry is struggling to keep up. NATO focuses its research and development efforts on nine areas: artificial intelligence (AI), autonomous systems, quantum technologies, biotechnology/human enhancement technologies, space, hypersonic systems, novel materials and manufacturing, energy and propulsion and next-generation communications networks (NATO, 2024). The principles and theories of warfare that have long remained unchanged are also changing. This essay focuses on current advanced technologies at the tactical level. The essay focuses on tactical-level technologies that we see on the battlefield today, such as drones, helmet cameras, bue force trackers, and battlefield command and control systems, which are reshaping the ways of warfare and changing the principles of command and control (C2) that have remained unchanged for decades. The question has rightly arisen whether the philosophy of mission control, which we consider the cornerstone of our military leadership today, can survive on the new technologically advanced battlefield? On the battlefield, the main effort of technological development has focused on developing situational awareness. Mission command emphasises disciplined initiative and decentralised decision-making. This philosophy was designed to overcome the uncertainty that prevails on the battlefield. (*ADP 6-0, 2019*). As Clausewitz said in his book Vom Kriege, uncertainty is one of the main aspects of the nature of war. While modern technologies provide the commander with good situational awareness and modern means of communication with his units, these means can also jeopardise the execution of mission command.

This essay argues that the technologies in use significantly increase situational awareness and improve communication capabilities but challenge the implementation of mission command and lead back to traditional command tactics (*befehlstaktik*). The technologies discussed in the essay, such as blue force trackers, live battlefield video on the commander's screen, battlefield control systems, and communications systems, create a complex environment in which the implementation of mission commands is simultaneously supported and threatened. The essay examines how these technologies can lead to micromanagement, information overload, risk aversion, and information- and technology dependency, which can undermine the foundations and principles of mission command.

Furthermore, this essay examines how mission command is handled in different branches of the military, the differences in balancing centralised control and decentralised execution, and their influence on C2 systems. It highlights differences and deviations from traditional mission command with reasoning. By analysing these challenges and attempting to find solutions to overcome them, this paper contributes to the existing discourse of military leadership on adapting to a changing technological environment while maintaining the core principles of mission command without neglecting technological development.

Essence of mission command

This chapter identifies the core characteristics of mission command and briefly outlines the effects of technology on these core characteristics. According to ADP 6-0, mission command has several key principles: mutual trust, shared understanding, commander's intent, mission orders, disciplined initiative, and risk acceptance. (*ADP 6-0, 2019*). In the following analysis, we will use these same principles and examine whether there is any information in the literature about how chosen technologies may erode these principles.

Mutual trust

It allows people to avoid attrition between each other and concentrate on the enemy. Mutual trust is based on personal qualities, such as professional competence, character, and commitment, and relies on a common background, education, understanding of doctrine, and a common language for operations. Trust can't be built instantly; it is created over time by sharing the same experiences. ADP 6-0 does not speculate how much time it may require. Many examples show how technologies can most significantly affect mutual trust and self-confidence. There are examples in the literature of how technologies can facilitate several trust- and self-confident-destroying activities, such as micromanagement and overcontrol (Lindh, 2022).

Shared understanding

Successful task performance requires a common understanding of the operational environment, the operation's objective, the problems and the ways to solve them. These are the basis for unity of effort and trust (*ADP 6-0, 2019*). In a battalion, a common understanding is developed due to staff work. Following the commander's instructions, the staff analyses either the order or the situation that has arisen and assesses the task, the environment, and the enemy and their impact on the task. This creates a common understanding during the task, which is shared with subordinates by issuing orders and confirmed through back briefing or rehearsal (Holmes, 2012).To maintain a common understanding, the commander must communicate to maintain situational awareness, resolve any misunderstandings that may arise, and assess the task's progress. This means there is constant cooperation, up and down (*ADP 6-0, 2019*). Constant communication can lead to information overload. That situation is where the amount of information becomes too big, and the staff cannot process it (Lindh, 2022). Additionally, the constant habit of communicating and receiving confirmation of one's actions and assessments from one's superior can lead to a situation where, without it, one can no longer cope in a situation where technology fails (Bollmann, Heltberg, 2023). It highlights another set of threats to mission command: information overload, overreliance on information and technology resilience.

A commander’s intent and mission-type orders

Mission-type orders are essential parts of the practice of mission command. The use of the commander's intent and mission-type orders is a common practice in the Estonian Defence Forces, as has also been shown by relevant studies (Sarap, Puusepp, Haas, Mumm, Lille, 2024). The mission-type order and the commander's intention are strongly related because, above all, the commander's intention and the great freedom of action to achieve the commander's desired goal make the order a mission-centric order (Harvard, 2013). Otherwise, today's technology does not affect mission-type orders and the commander's intent.

Disciplined initiative

Discipline initiative refers to the courage of a subordinate to make decisions and change their original plan to achieve the goals outlined in the commander's intent. This need usually arises when the environment changes compared to what was considered in the original plan. Either the opponent behaves differently than predicted, or the terrain does not correspond to the original assessment, which prevents the plan from being implemented. The primary need to show initiative comes from the urgency of the situation. The unit commander does not have time to brief his commander on the situation and coordinate actions (*ADP 6-0, 2019*). According to the literature, online data can lead to centralised decision-making, reducing the adaptive capacity of decision-making and increasing risk aversion (Bryant, Smith, 2013). Risk aversion is related to the following mission command principle: risk acceptance.

Risk acceptance

Risk is an integral part of warfare. Commanders work with subordinates to analyse and mitigate risks, balancing the threat to the unit against the potential benefits. When making decisions, commanders consider the importance of objectives, the time available, and the expected losses. The most incredible opportunities may arise from courses of action with the greatest risks, such as committing significant forces to a costly frontal assault to enable encirclement. While caution is necessary, excessive risk aversion can hinder mission accomplishment. Mission command requires acceptable risk management, initiative, and decisive action, even in uncertain situations. Commanders should avoid gambling by making decisions without reasonable information about the possible outcomes. Instead, they should carefully assess risks, minimise hazards where possible, and accept calculated risks to accomplish the mission (*ADP 6-0, 2019*). Some authors have found that the military does not fully embrace mission command in the garrison because leaders are risk-averse and lack trust in their subordinates. This distrust only deepens in a tactical situation. Risk tolerance is related to control and decision-making. Control, however, is an inherent part of military leadership, which modern management technologies only enhance. However, more significant control biases leadership toward centralisation, which, as previously stated, does not support the implementation of the mission command philosophy in the military and increases the risk-averseness of subordinate leaders (Orsi 2019).

Potential pitfalls from technologies to mission command

We will now look closer at the previously identified threats to mission command posed by emerging technologies. Some of these threats can undermine several mission command principles and are, therefore, particularly dangerous, and their avoidance should be given great attention in the training of military leaders.

Micromanagement, overcontrol and risk aversion

Micromanagement will hinder the speed of the decision-making process, disrupt mutual understanding and mutual trust, and reduce the subcommander's creativity and overall performance (DeLeon, Tripodi 2022). It will also hamper the ability to learn and develop. Employers develop most when solving "stretch assignments", autonomously solving tasks beyond their current skills and knowledge. Delegation of tasks, authorities, and decision-making allows subordinates to grow responsibility and be part of achieving organisational goals (DeLeon, Tripodi, 2022). All three technologies, blue force trackers, live feed, contemporary communication and battle management systems, tempt commanders to overcontrol or overtake the responsibilities of subordinates (Nilsson 2020). In Operation Iraqi Freedom, where BFT was widely in use, it was seen as a punishment. Platoons who were not aggressive enough were forced to wear BFT. Furthermore, direct ordering from many levels of higher commanders occurred (Salvi, Spagnoletti 2022). 1st Marine Division's entire chain of command was observed by higher command. This means that the autonomy of the 1 Division commander was apparent. Actual decisions were made by higher command (Simonetti, Tripodi, 2020). That example illustrates Boyd's statement that the breakdown of the implicit communication and trust that defines "mission command" creates "confusion and disorganisation that hinders robust solution-oriented action and increases friction, which is the opposite of what was intended to be achieved by increasing the freedom of action of small forces (Boyd, 1987). Despite that, the US Armed Forces have prioritised developing network-centric warfare systems (NCW), allowing information exchange between units in every domain linked to the system (*The Implementation of Network-centric Warfare*, 2005). This sensor-shooter-decision-maker network has created, in many cases, "tactical generals" who spend several hours watching live feeds of the single weapon system, thus implementing centralised control and micromanagement instead of principles of mission command (Singer, 2009). So, there is a contradiction between the adopted command philosophy that encourages delegation of power to lower levels of command and, on the other hand, building systems that allow the practice of central command and control (Simonetti, Tripodi, 2020). Resisting this requires effort but is possible through training and awareness of the problem. The following section will move to the next threat and discuss information overload.

Information overload

This threat has arisen with the development of battle management systems, and information overload describes contemporary warfighting (Thibodeau, 2020). The essay's author has personally experienced the information overload in the battalion's forward command post caused by the reconnaissance drone's introduction. The battalion's forward command post set tasks for the reconnaissance drone. The commander decided to implement or change the battle plan based on the information received. Furthermore, the information received on identified targets allowed the fire support officer to plan their destruction. This created a flat organisational structure, where the classic sensor, decision-maker and shooter structure was created. At such a detailed level of information exchange, even one subscriber created an information overload for the battalion headquarters. Some studies argue that information overload can, in turn, cause paralysis and reduce mission effectiveness (Bollmann, Heltberg, 2023). The reason for decreased effectiveness is the commander's ability to make sound decisions on time (Thibodeau, 2020). Information processing should be distributed between nodes to avoid information overload. The research used in the essay discovered that the imbalance of situational awareness in organisations still exists. Those with high situational awareness have ties with others with high situational awareness (Buchler et al., 2016). General McChrystal was trying to overcome that tendency by having weekly meetings with a broad spectrum audience, not only units under his command but also other key players in the theatre. He also distributed his authority by allowing lower-level commanders to launch an attack or arrest when conditions were met (McChrystal, Collins, Silverman, Fussell, 2015). Sharing the burden of receiving and processing information also requires sharing authority. But this is not always possible. The lowest level that requires a joint warfighting capability is the battalion. A missile strike order passes through a formal hierarchical structure through six levels of command before finally reaching the decision maker who authorises the order to fire (Zelaya, Keeley, 2020). The same applies to high-impact precision weapon systems. Some authors stated that the level of centralisation should be in correlation with asset availability. If an asset is widely available, its control could be decentralised. For air assets, the most suitable is to practice centralised command and decentralised execution (Harvard, 2013). It's challenging to discuss delegating the authority to use the Storm Shadow rocket, given that fewer than a thousand are believed to be in the possession of the UK (Pfeifer, Nilsson, 2024). This is not the last challenge related to technology. Increasingly, I see a lack of critical thinking, interpretive skills for what is seen on and off the screen, and a lack of courage to make decisions without technological aids. This opens a discussion about the following section: an overreliance on information and technological resilience.

Information overreliance and technological resilience

The new generation entering the military has grown up within the digital world. It is unimaginable to establish C2 without digital assets. It is commonly agreed that advanced technologies are taking annoying tasks away from us, such as copying battle graphics from higher orders. However, there is also the risk that people over-rely on technology (Bollmann, Heltberg, 2023). Recent studies show that AI significantly reduces people's creativity and ability to think critically and find solutions independently. AI is not yet inevitable. Using AI may hide many failures like AI hallucination, algorithmic bias, and plagiarism. (Zhai, Wibowo, Li, 2024). The same tendencies apply to the examples selected in the work. Dependence or overreliance can be on the information provided by different sources, such as the Blue Force Tracker or video feed. Commanders start to depend on detailed information and lose their ability to decide in uncertain situations. Technology has become a crystal ball that sees the future and, simultaneously, a silver bullet that finds answers to the disappearance of the future it has seen. This has made leaders hesitant and indecisive when technological tools do not support them (Bollmann, Heltberg, 2023).

As mentioned, NCW allows us to minimise the so-called fog of war. That may result in moving back to the traditional C2 model, where command and control are seen as more unidirectional (Simonetti, Tripodi, 2020). But to be efficient in this model, situational awareness of the commander is crucial. Therefore, the sustainability and reliability of those systems are very vital. Nevertheless, history provides several examples of how trusted and relied-on technology has failed. In August 2017, the US Navy destroyer John S. McCain and the Liberian tanker Alnic MC collided when the US Navy ship sharply turned to port. The investigation determined that the Integrated Bridge and Navigation System was a major contributor to the accident. This system contained several design flaws that, combined with human error, led to a loss of steering control and a collision with another vessel, resulting in the deaths of ten U.S. sailors. (Ding, 2024).

In August 2021, coalition forces conducted an evacuation operation under U.S. leadership after the Taliban came to power. The U.S. Air Force used a software tool developed by Kessel Run to coordinate the operation. The software was a key part of the evacuation, helping to plan aircraft arrivals and departures from Hamid Karzai International Airport. However, a software glitch occurred during the operation, as the chaos and the high demand for evacuation significantly increased the number of people requiring evacuation and the number of flights required. However, this number exceeded the software's planned capacity, and the software crashed (Ding, 2024). It can be indirectly said that this crash resulted in the deaths of at least 182 people in the ISIS-K attack. The software crash could have been prevented by implementing specific development processes, but this was not done (Ding 2023).

The most recent example is from Israel. Hamas was breaking the smart fence with low-tech assets and found a way to outplay Iron Dome. Israeli overreliance on technology had a significant role in it. Hamas was destroying generators of communication towers with drones that were carrying explosive charges. That disabled the communication between sensors and personnel controlling the sensors and the remote machinegun turrets. Furthermore, the cameras and ammunition boxes of those turrets were shot with sniper fire. This is how the smart fence was neutralised, and the initial surprise was achieved. The capacity of Iron Dome was overloaded by launching 3000 rockets within 20 minutes. The capacity of the Iron Dome missile system was tested several times before the actual attack (Carhidi, 2023). These are some examples of overreliance on technology. Even if they are not entirely about C2 systems, the same logic can apply to technology that is used for C2. Technology can be outplayed by simple means, as we witnessed in Ukraine in 2023 when Russia started to use cheap Iranian drones in large quantities. Ukraine was using many expensive Western-made air defence weapons to repel them (Minnik, 2023). Electronic warfare against communication systems, which are widely used in Ukraine, is the primary concern of communication means. Electronic warfare units jammed Russian drones before the attack, taking away situational awareness from commanders, and then communication systems were also suppressed to cut off control (Hambling, 2024). There have been discussions about using nuclear high-altitude electromagnetic pulse (HEMP). Of course, the use of any atomic weapon may cause escalation that causes a third world war. But cannot be overruled. The use of HEMP in populated areas has severe consequences. Exploring it remotely could destroy C2 without collateral damage among people. That could easily knock out technology-dependent western or Ukrainian units (Pence, 2021). So, relying blindly on technology may lead to fatal consequences.

Psychological affection on decision-making

Several articles are available about the burden of junior officers, like platoon leaders and company commanders who lost their soldiers under their command. A squad leader blames himself for the deaths of his men after they hit an improvised explosive device, as he was the one who chose the route they hit. Losing men can lead to a loss of courage and indecision, which can have even more fatal consequences. However, there is no research on how it influences higher commanders and decision-making. Research shows that war trauma can occur for a variety of reasons. Still, the most common causes may be direct participation in combat, giving orders and instructions that caused death or suffering, causing death, injury or suffering, or directly experiencing it (Fielding, 2023). As mentioned earlier, the battlefield has also changed for the commander. The killed enemy is no longer just an anonymous number. Still, often, senior officers also experience first-hand the horrors of battle through video footage, including the collateral casualties of combat and the deaths of civilians, women and even children. A US Air Force drone pilot admitted that his mental and physical health deteriorated during the war. He felt like a “legion of the dead” he had killed were chasing him. It led him to consider suicide (Zust, Krauss, 2019). Even in combat situations, commanders must sustain their decision-making resilience. It is described as the ability to remain calm and calculative in intense situations and make sound decisions, finding practical and effective solutions to problems (Badiu, Țică, 2023). Modern technology has made it much more difficult for a commander to distance himself from combat operations, which is why the commander also experiences more significant psychological pressure than before. There are currently no studies on this topic. Still, based on the previous information, there is reason to believe that these connections exist and that real-time battlefield monitoring negatively affects the leader's decision-making ability, similar to officers participating in direct combat.

Improvements to mission command through technology

Although the literature provides an overview of several adverse effects that modern technology brings to management, many positive aspects can be summarised as improved situational awareness. Enhanced situational awareness also entails risks that must be mitigated so that they do not undermine leadership effectiveness.

Enhanced Situational Awareness

The main idea of mission command is to delegate power to subunits because they have higher situational awareness. If units have a goal, they can choose suitable ways to achieve it and include necessary forces in their plan. This leadership philosophy helps to overcome the uncertainty caused by the “fog” of war. Some experiments in the Norwegian Navy show that this is not the case for the Navy. A more rigid and order-based command style was performed in the case of a commander receiving a task where some uncertainties appeared (Krabberød, 2014). So, the purpose of practising mission command did not meet the expected outcome in that case. On the other hand, infantry has trusted the decentralised execution to bigger units – battalion, brigade, or higher. Contemporary technologies improve higher echelon situational awareness, whose command posts are far from the front. Now, generals can oversee the battlefield, see from the screen where all the friendly units are located, and make better decisions (Salvi, Spagnoletti 2022). Of course, it is a tremendous change for the platoon- and company commander to have an overview of the situation from the drone. According to some researchers, also manoeuvring units benefit significantly through more precise C2. However, network-centric warfare (NCW) compresses tactical and operational levels into the same space. It allows commanders to make exact and sound tactical decisions instead of deciding only at the operational level. Inevitably, it drives warfare back to the classical hierarchical command model. Units in the field will have increased situational awareness but have lost their autonomy and initiative (Simonetti, Tripodi, 2020). It may even lead to de-responsibilisation. Tactical units don't feel responsible for the situation; instead, they count on advice or orders from a higher commander (Salvi, Spagnoletti, 2022), a stereotype of soldiers from the Great World War. Following only orders and not thinking. So, the small units can benefit only from assets that are subordinated to them. Blue force trackers, battle management, and communication systems are helpful to higher command but tend to direct commanders back toward command tactics (*befehlstaktik*).

Improved Communication and Coordination

Temporary battle management and communication systems have sped up the communication between units. There is no need to spell the reports or copy and draw the maps on paper. Contemporary technologies allow headquarters to share written reports, plans, and even the current location of units on a digital map (Bollmann, Heltberg, 2023). Global communication allows the commander to interact with the tactical unit on the battlefield directly. It reduces inevitable distortion and delays when information passes a hierarchical structure. Especially reaping the benefit of it on joint warfare-level command. The use of high-precision and standoff-weapons systems is much faster and better integrated. It allows tactical-level commanders to have an overview of the overall situation and, therefore, to make better decisions. On the other hand, challenges with information overload could be faced now because smaller headquarters cannot analyse such an amount of information (Simonetti, Tripodi, 2020). Furthermore, it is argued that improved communication does not favour mission command of small units; instead, it guides the army back to a centralised command style. Lower-level commanders are losing their initiative, and higher-level commanders may turn to “tactical generals” (Johnson, 2023).

Exceptions and deviations from mission command

Not all military branches emphasise mission command in the way the Army does. US Air Force doctrine covers mission command indirectly and states that the Air Force practices decentralised execution with mission-type orders. Airman sees that situational awareness may differ during the operation. When the wing commander gives an order to the squadron commander, they have higher situational awareness. But it will probably change during the mission. The Squadron commander will have better situational awareness, and the higher command must accept the squadron commander's decisions. Airmen see this kind of centralised control and decentralised execution as the distinction of the Air Force (Harvard 2013). The reason is that the Air Force delivers theatre or sometimes even global effects. Airpower is projected within all Joint Area of Operation (JOA) to meet the requirements and priorities of the Joint Force Commander (JFC). Tactical tasks like close air support require a much more decentralised approach than space or nuclear operations controlled by the highest level. (Harvard, 2013). So, the C2 style depends on the situation, and mission command is more likely to be implemented at the tactical level.

US Special Operation Forces do not explicitly mention mission command in their doctrine. Instead, they see that the structure of command is the key aspect. Many authors see that decentralised command cannot be achieved within a hierarchical C2 structure (Bury, 2022). The desired C2 structure is described as networked by retired general Stanly McChrystal in his books (McChrystal et al., 2015) It means that military forces should be organised like Al-Qaeda was formed in Afghanistan (Arendt, 2013) They will get training, resources from the umbrella organisation, and the overall aim or goal. However, they are fully autonomous in choosing targets or how to execute the task (Buchler et al., 2016). The network type of organisation is not considered the best in every situation. It is more suitable for solving complex and wicked problems. It is too time-consuming and resource-costly to solve simple tasks (Liias, 2021).

US Marine Corps doctrine sees the possibility of exercising detailed C2 and mission command. They see that the C2 type will depend on the situation and, in reality, is most likely a combination of both styles (Harvard, 2013). This opinion is also in line with general organisation theory. Different type of tasks requires different leadership.
US Navy doctrine emphasises mission command as a key tenet of their leadership style. Its roots are deep in issues with the poor communications the navy has overcome in the contemporary era. But still, it is sitting in their doctrine (Harvard, 2013). It may vary by country and unit, but it is not an effortless command style to practice, as the experiment in the Norwegian Navy showed. Per Navy Warfare Publication 3-32, similarly to the Army, the commander's will or guidance is provided through the commander's intent, that is, saying what needs to be achieved and how it is achieved is the subcommander to decide (Krabberød, 2014).

The different understanding of mission command may also be why battlefield management systems must be suitable for combined arms combat, where those branches of the military that define the mission command differently also participate. Understandably, there is a desire to gain central control over a single weapon system since they create strategic effects. However, this has directed the development of battle management systems so that infantry must make additional efforts to maintain mission command leadership philosophy.

How to overcome threats to Mission Command?

There are many discussions on how to improve the unit performance of C2 in the age of digitalisation. As described in the previous paragraphs, there are many pitfalls. The ways to overcome the shortfall are divided into two main categories: training and education and the resilience of the technology. Training is a broad topic that can significantly diminish the threat of falling into the trap of potential pitfalls.

Training is mentioned widely in the literature. It covers the importance of training at the lowest level until the joint level. Krulak describes in his books the importance of recruitment, training, and mentorship that allows junior leaders to step up and become “strategic corporal”. He did not describe explicitly mission command training, but rather additional personal skills to soldiers' basic training like cultural sensitivity, media awareness, mediation skills, linguistic competence, how to use more sophisticated weapon systems and sensors that were in use, and small group tactics (Annis, 2020). As mentioned before, advanced technologies support network-centric warfare, and they are tempting to micromanage and overcontrol, which are hampering building trust. Commanders should create a training environment to foster and nurture junior commanders' decision-making to overcome that. Encouraging them to make fast decisions in uncertain situations and accept their failures (Nilsson, 2021). The precondition for success is that commanders of all levels be present during the training. For example, company commanders can practice giving their platoons freedom of action, showing initiative, and accepting failure. However, this is useless if the battalion commander starts instructing platoons by bypassing the company commander or does not give the company commander a mission-type order that does not allow for extending mission control to a lower level.

Training programs should focus on developing cognitive skills like fast information processing and pattern recognition to orientate faster. (Thibodeau, 2020). It may also require reorganising the intelligence and operation structure to divide the information flow between the nodes to distribute the workload (Horlings, Lindelauf, Rietjens, 2023). For example, the Estonian brigade commander does not follow all the information but rather delegates it to subject matter experts. Enemy overall picture and advice to the commander will be provided from the forward command post. Operation-related information is also divided between the engineer-, and the fire support officer in the forward command post. The rear command post is collecting information related to sustainability. It is similar in many Western and US units, according to FM 6-0. It means that information flow is already distributed. Information overflow endangers not only humans but also communication and battle management systems. That takes us to technological resilience.

The threat to technology is a harsh environment that can damage communication systems and data overload. According to studies conducted by the Estonian Military Academy, advanced course students at the tactical level of the units operate at the edge of their communication systems' capability (Hunt, 2020). Not only is the tactical level suffering under increased data flow. Demand for bandwidth on military satellites is much higher than the sources available. And the trend is rising. Countries are looking for possibilities to use commercial satellites for less critical communications (Turnbull, 2013). Therefore, it is essential to have emergency systems that you can use as backup. It is common for Estonians to have the digital battle management system KOLT as the primary C2 system (Unt, 2020). KOLT has another application interface, TOORU, for brigade-level fire coordination (Päären, 2024). But those systems should be backed up by the analogue system - situational overview map and communication via voice. This is vital to avoid the collapse of C2 when battle management systems don’t work or have been suppressed by the enemy.

Conclusion

Summarising the previous analysis, modern technologies have changed the battlefield and its management. Video images reaching the headquarters directly from the battlefield, devices for determining the location of friendly units, and battle management systems that allow communication several levels down can significantly improve commanders' situational awareness. However, simultaneously, they threaten the still prevailing leadership philosophy, the mission command philosophy. The implementation of mission command philosophy varies depending on the service. The fewer the means that create effects and the more critical the impact that the means achieve, the more centrally coordinated the use of these means is. Such services include air, space, and special operations forces, which implement strategic effects. A flat command structure poses several dangers for other military branches, such as micromanagement and information overload. In addition, modern technologies can create dependence and overreliance on technology. These threats can undermine the foundations of mission command philosophy, which are mutual trust, shared understanding, disciplined initiative, and acceptance of risk and failure. The primary solution to mitigate these risks and mitigate their consequences is training and increasing the reliability of technology. Units must be trained to recognise and overcome the threats that lie ahead. Training must create a realistic environment that fosters mutual trust, allows for disciplined initiative, and trains the commander to trust his subordinates, accept their adopted course of action, and encourage them to strive forward in the event of failure. Second, training must be practised in a high-tech environment, which is the inevitable future. This allows staff to develop the necessary changes to share information flows that support subordinates' freedom of action and contribute to implementing the mission command philosophy. Finally, systems must be more resilient to withstand harsh environments and increased workloads while maintaining the flexibility to transition to more primitive means if technology fails. Ultimately, the survival of mission command in an era of evolving technologies depends on leaders' ability to find a balance between exploiting the benefits of technological advances whilst protecting the fundamental principles of mission command. Only through conscious effort and adaptation can soldiers harness the full potential of technology without sacrificing the flexibility, resilience, and initiative that are the foundation of effective military leadership.

Bibliography

ADP 6-0, 2019. [Online]. [Cited: 13 November 2024]. https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN34403-ADP_6-0-000-WEB-3.pdf

ANNIS, Franklin. 2020. Krulak Revisited: The Three-Block War, Strategic Corporals, and the Future Battlefield. *Modern War Institute.* [Online]. 3 February 2020. [Cited: 13 November 2024]. https://mwi.westpoint.edu/krulak-revisited-three-block-war-strategic-corporals-future-battlefield/

ARENDT, Hannah. 2013. General Stanley McChrystal: My Share of the Task. [Online]. 8 March 2013. [Cited: 11 November 2024]. https://hac.bard.edu/amor-mundi/general-stanley-mcchrystal-my-share-of-the-task-2013-03-08

BADIU, Marius Iulian and ȚICĂ, Laura-Alexandra. 2023. The resilience of the military leader – defining traits and its ability to influence the operational environment. Bulletin of "Carol I" National Defence University. [Online]. 7 July 2023. Vol. 12, no. 2, pp. 134–141. [Cited: 31 October 2024]. DOI 10.53477/2284-9378-23-25.

BOLLMANN, Anders and HELTBERG, Therese. 2023. The Strategic Corporal, the Tactical General, and the Digital Coup d'oeil – Military Decision-Making and

Organizational Competences in Future Military Operations. Scandinavian Journal of Military Studies. 21 August 2023. Vol. 6, pp. 151–168. DOI 10.31374/sjms.190.

BOYD, John. 1987. Organic Design for Command and Control. [Online]. 1987. [Cited: 2 August 2025]. https://www.coljohnboyd.com/static/documents/1992-08__Boyd_John_R__Conceptual_Spiral__PPT-PDF.pdf

BRYANT, David J. and SMITH, David G. 2013. Impact of blue force tracking on combat identification judgments. *Human Factors*. February 2013. Vol. 55, no. 1, pp. 75–89. DOI 10.1177/0018720812451595.

BUCHLER, Norbou, FITZHUGH, Sean M., MARUSICH, Laura R., UNGVARSKY, Diane M., LEBIERE, Christian, et al. 2016. Mission Command in the Age of Network-Enabled Operations: Social Network Analysis of Information Sharing and Situation Awareness. Frontiers in Psychology. 2016. Vol. 7, pp. 937. DOI 10.3389/fpsyg.2016.00937.

BURY, Patrick. 2022. US Special Forces transformation: post-Fordism and the limits of networked warfare. *International Affairs.* [Online]. 7 March 2022. Vol. 98, no. 2, pp. 587–607. [Cited: 11 November 2024]. DOI 10.1093/ia/iiab213.

CARHIDI, Vincent. 2023. The October 7 Hamas attack: An Israeli overreliance on technology? Middle East Institute. [Online]. 23 October 2023. [Cited: 30 October 2024]. https://www.mei.edu/publications/october-7-hamas-attack-israeli-overreliance-technology

DELEON, Justin T. and TRIPODI, Paolo G. 2022. Eliminating Micromanagement and Embracing Mission Command. [Online]. 10 January 2022. [Cited: 27 September 2024]. https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/September-October-2022/DeLeon-Tripodi/

DING, Jeffrey. 2023. Machine Failing: System Acquisition, Software Development, and Military Accidents. 1 July 2023.

DING, Jeffrey. 2024. Machine Failing: How Systems Acquisition and Software Development Flaws Contribute to Military Accidents. Texas National Security Review. [Online]. 17 October 2024. [Cited: 15 February 2025]. https://tnsr.org/2024/10/machine-failing-how-systems-acquisition-and-software-development-flaws-contribute-to-military-accidents/

FIELDING, Sarah. 2023. War Trauma. Charlie Health. [Online]. 15 August 2023. [Cited: 22 February 2025]. https://www.charliehealth.com/post/war-trauma-psychological-consequences-of-war

HAMBLING, David. 2024. Ukraine's Kursk Offensive Blitzed Russia With Electronic Warfare And Drones. *Forbes*. [Online]. August 2024. [Cited: 19 February 2025]. https://www.forbes.com/sites/davidhambling/2024/08/09/ukraines-kursk-offensive-blitzed-russia-with-electronic-warfare-and-drones/

HARVARD, James W. 2013. Airmen and Mission Command. Air & Space Power Journal. [Online]. 4 January 2013. https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Volume-27_Issue-2/F-Harvard.pdf#:~:text=understand%20the%20relationship%20between%20mission%20command%20and%20the%20Air%20Force

HOLMES, Chuck. 2012. The Military Decision Making Process: Tips & Guidance. [Online]. 27 August 2012. [Cited: 1 February 2025]. https://www.part-time-commander.com/military-decision-making-process/

HORLINGS, Tess, LINDELAUF, Roy and RIETJENS, Sebastiaan. 2023. "Battling information overload in military intelligence & security organisations", in Towards a Data-Driven Military: A Multidisciplinary Perspective, eds. Peter Pijpers, Mark Voskuijl and Robert Beeres (Leiden, Leiden University Press, 2023). In: pp. 221–236. ISBN 978-90-8728-408-4.

HUNT, Henri. 2020. Jalaväebrigaadi taktikalise sidevõrgu andmeside läbilaske vajadus 1. Jalaväebrigaadi näitel. Estonian military Academy.

JOHNSON, James. 2023. Automating the OODA loop in the age of intelligent machines: reaffirming the role of humans in command-and-control decision-making in the digital age. Defence Studies. [Online]. 2 January 2023. Vol. 23, no. 1, pp. 43–67. [Cited: 28 September 2024]. DOI 10.1080/14702436.2022.2102486.

KRABBERØD, Tommy. 2014. Task Uncertainty and Mission Command in a Naval Context. Small Group Research. [Online]. 1 August 2014. Vol. 45, no. 4, pp. 416–434. [Cited: 11 November 2024]. DOI 10.1177/1046496414532955.

LIIAS, Taavi. 2021. The Command and Control of Estonia's Integrated Defence on the Regional Level: The Network Organization. [Online]. Estonian Military Academy.

https://www.etis.ee/portal/mentorships/display/e2d8ac01-e011-4a4d-8a41-c64da2972c05

LINDH, Philip. 2022. Military Leadership and Technology. Swedish Defence Universty, Department of Security, Strategy and Leadership. 3 January 2022.

MCCHRYSTAL, General Stanley, COLLINS, Tantum, SILVERMAN, David and FUSSELL, Chris. 2015. Team of Teams: New Rules of Engagement for a Complex World. Penguin. ISBN 978-0-698-17851-9. Google-Books-ID: iFr2AwAAQBAJ

MINNIK, Taavi. 2023. „Need kurnavad meie õhutõrje välja.“ Iraani kamikaze-droonid põhjustavad Ukrainale suurt peavalu. Kuidas nendega võidelda? Forte. [Online]. 23 October 2023. [Cited: 30 October 2024]. https://forte.delfi.ee/artikkel/120235832/need-kurnavad-meie-ohutorje-valja-iraani-kamikaze-droonid-pohjustavad-ukrainale-suurt-peavalu-kuidas-nendega-voidelda

NATO. 2024. Emerging and disruptive technologies. *NATO*. [Online]. 8 August 2024. [Cited: 10 March 2025]. https://www.nato.int/cps/en/natohq/topics_184303.htm

NILSSON, Niklas. 2021. Mission Command in a Modern Military Context. Journal on Baltic Security. 13 May 2021. Vol. 7. DOI 10.2478/jobs-2021-0001.

ORSI, Doug and MUNDELL, Bobby. 2019. Will new doctrine fix mission command? War Room - U.S. Army War College. [Online]. 9 October 2019. [Cited: 8 February 2025]. https://warroom.armywarcollege.edu/articles/new-doctrine-mission-command/

PÄÄREN, Mariliis. 2024. Kaitseväe Akadeemia andis küberväejuhatusele üle teadusprojekti raames loodud Tooru programmi – Kaitseväe Akadeemia. [Online]. 16 January 2024. [Cited: 21 November 2024]. https://www.kvak.ee/uudised/kaitsevae-akadeemia-andis-kubervaejuhatusele-ule-teadusprojekti-raames-loodud-tooru-programmi/

PENCE, Scott. 2021. Fighting as Intended: The Case for Austere Communications. National Defense University Press. [Online]. 6 January 2021. [Cited: 30 October 2024]. https://ndupress.ndu.edu/Media/News/News-Article-View/article/2679508/fighting-as-intended-the-case-for-austere-communications/https%3A%2F%2Fndupress.ndu.edu%2FMedia%2FNews%2FNews-Article-View%2FArticle%2F2679508%2Ffighting-as-intended-the-case-for-austere-communications%2F

PFEIFER, Sylvia and NILSSON, Patricia. 2024. Why Germany's Taurus is Europe's most-wanted long-range missile. [Online]. 15 March 2024. [Cited: 29 October 2024]. https://www.ft.com/content/09f2ec36-de20-4ea2-abf2-49f70275c521

RISTYAWAN, Mochammad Ridwan, PUTRO, Utomo Sarjono and SIALLAGAN, Manahan. 2023. Decision making mechanism in resource based theory: A literature review, synthesis, and future research. Cogent Business & Management. [Online]. 12 December 2023. Vol. 10, no. 2, pp. 2247217. [Cited: 29 October 2024]. DOI 10.1080/23311975.2023.2247217.

SARAP, Indrek, PUUSEPP, Mattias, HAAS, Ermo, MUMM, Elvis and LILLE, Meelis. 2024. Ülema kavatsus ja selle rakendamine kaitseväes. [Online]. 13 March 2024. [Cited: 8 February 2025]. https://issuu.com/sodur/docs/s6dur_1_24_issuu

SIMONETTI, Rosario M. and TRIPODI, Paolo. 2020. Automation and the Future of Command and Control: The End of Auftragstaktik? Journal of Advanced Military Studies. [Online]. 15 July 2020. Vol. 11, no. 1, pp. 127–146. [Cited: 20 October 2024]. DOI 10.21140/mcuj.2020110106.

SINGER, Peter W. 2009. Tactical Generals: Leaders, Technology, and the Perils. Brookings. [Online]. 7 July 2009. [Cited: 28 September 2024]. https://www.brookings.edu/articles/tactical-generals-leaders-technology-and-the-perils/

The Implementation of Network-centric Warfare, 2005. Force Transformation, Office of the Secretary of Defense. ISBN 978-0-16-073266-9. Google-Books-ID: Tq4xm7g8XpwC

THIBODEAU, Daniel. 2020. Information Overload: A Warfighter's Challenge. *Canadian Forces College*. 1 January 2020.

TURNBULL, Grant. 2013. Data overload: satellite communications on the battlefield. Airforce Technology. [Online]. 26 November 2013. [Cited: 16 November 2024]. https://www.airforce-technology.com/features/feature-data-overload-satellite-communications-battlefield/

UNT, Hare. 2020. Sõjalise kohaviitevõrgustiku kasutuselevõtmise võimalikkus ühtse standardina Eesti jõustruktuurides, maismaal asukoha määramiseks. [Online]. The Estonian Academy of Security Sciences.

https://digiriiul.sisekaitse.ee/bitstream/handle/123456789/2491/2020_Unt.pdf?sequence=1

ZELAYA, David and KEELEY, Nicholas. 2020. The Input-Output Problem: Managing the Military's Big Data in the Age of AI. War on the Rocks. [Online]. 13 February 2020. [Cited: 7 October 2024]. https://warontherocks.com/2020/02/the-input-output-problem-managing-the-militarys-big-data-in-the-age-of-ai/

ZHAI, Chunpeng, WIBOWO, Santoso and LI, Lily D. 2024. The effects of over-reliance on AI dialogue systems on students' cognitive abilities: a systematic review. Smart Learning Environments. [Online]. 18 June 2024. Vol. 11, no. 1, pp. 28. [Cited: 15 November 2024]. DOI 10.1186/s40561-024-00316-7.

ZUST, Jeffrey and KRAUSS, Stephen. 2019. Force Protection from Moral Injury: Three Objectives for Military Leaders. National Defense University Press. [Online]. 2019. [Cited: 22 February 2025]. https://ndupress.ndu.edu/Media/News/News-Article-View/Article/1737148/force-protection-from-moral-injury-three-objectives-for-military-leaders/https%3A%2F%2Fndupress.ndu.edu%2FMedia%2FNews%2FNews-Article-View%2FArticle%2F1737148%2Fforce-protection-from-moral-injury-three-objectives-for-military-leaders%2F

LTC Alexandra Möckel. Howitzers vs. FPV-UAV – The Future of Tube Artillery in Multi-Domain Operations

The Future of Tube Artillery in Multi-Domain Operations

In recent decades, with the end of the Cold War, Western nations have greatly reduced their armed forces and restructured them to meet the challenges of the time, such as counterterrorism and stabilization operations. Artillery, in particular, has lost importance. Notably, the ability to fight with fire in deep areas has been neglected due to the focus on stabilization missions. The German Armed Forces, for example, reduced its artillery battalions to just four remaining over the past three decades. During the Cold War, the German Artillery had over 40,000 posts and comprised around 100 regiments, battalions, and independent batteries. (Geiger, 2023) In recent operations, like those in Kosovo and Afghanistan, Germany focused on counterinsurgency and peace support. The use of artillery was reduced to firing illumination ammunition as a show of force.

One reason was the realization that the conventional use of indirect fire caused too much collateral damage, especially in battles in urban areas amid civilian populations. For centuries, artillery fire was effective primarily due to its shells' explosive force and fragmentation. Artillery's strengths include its capability to penetrate deep into enemy lines, rapidly redirect the main concentration of fire, and create an area effect against unprotected targets.

The war in Ukraine signals the resurgence of high-intensity conflict and shows that artillery is still the king of the battlefield. It is responsible for most of the losses on both sides. (Grey, et al., 2024) The war has highlighted the need for investment in land-based fire capabilities. Like most Western Allies, the German Armed Forces has also recognized this change in relevance and is planning to increase the number of Artillery battalions to ten by 2035. According to the presentation of Lieutenant General Andreas Marlow, Vice Chief of the German Army, on 9th October 2024, these ten artillery battalions consist of one corps artillery battalion, two divisional artillery battalions, and seven brigade artillery battalions. After current plans, there will be rocket artillery systems with an extended range of up to 300 kilometers at the corps level. The two divisional artillery battalions will have tube and rocket artillery systems and should be able to detect and attack targets at up to 150 kilometers. The seven remaining artillery battalions are divided into four heavy and three medium artillery battalions and will be deployed at brigade level. All seven battalions are tube artillery. The four heavy ones will be equipped with the PzH 2000, and the three medium ones with the new RCH 155 wheeled howitzer, which has yet to be procured. (Geiger, 2024) In addition to the resurgence of artillery, there is another highly efficient and incredibly rapidly evolving player on the battlefield – armed drones. High speed, low cost, ease of procurement, and extreme flexibility of these new assets seem to overshadow traditional systems such as tube artillery. Should the restructuring and reconstruction efforts of the Bundeswehr, where possible, already be outdated?

This research paper seeks to address the question: Do howitzers still have a place in the digital landscape of the 21st century? The paper is organized into four distinct sections to explore this query systematically. The first section will elucidate the role of joint fires within multi-domain operations. The second section will provide a comprehensive analysis of the capabilities and limitations of both tube artillery and aerial drones, highlighting the comparisons between the two. To maintain a focused scope, particular emphasis will be placed on "First Person View" (FPV) drones and quadcopters, as they represent a significant evolution in battlefield dynamics and are actively utilized for fire support at the tactical level in the ongoing war in Ukraine. Information on drone warfare is limited due to its rapid evolution and operational secrecy. Consequently, research may rely on readily available information, potentially misrepresenting the reality of drone operations. While this analysis highlights the increasing importance of FPV drones, availability bias may influence these conclusions. Further research is needed to provide a more comprehensive picture of the military reality. In the concluding section, the paper will examine the future of tube artillery, identifying necessary adaptations and advancements. This research argues that although FPV UAVs pose substantial challenges to traditional tube artillery, howitzers will continue to play a vital role in multi-domain operations by embracing technological integration and adapting their operational functions. Ultimately, the paper will demonstrate howitzers have historically held, currently hold, and will continue to hold relevance in modern warfare.

The Role of Joint Fires in Multi-Domain Operations

With the amphibious operation Albion in World War I, Germany executed the first joint operation, which took place simultaneously in the three domains: land, sea, and air. Joint operations involve military actions in more than one domain, requiring multiple armed force branches to achieve military objectives. Since World War I, joint operations between the army, navy, and air force have become increasingly critical. These three domains have been the focus of NATO when planning and conducting its operations over the past decades. (Schnaubelt, 2023) Meanwhile, with the growth of the World Wide Web and the use of space, the domains of cyberspace and space have also become the focus of NATO and its planning process. While joint operations refer to the three traditional domains: land, sea, and air, multi-domain operations occur within the five domains: land, sea, air, cyberspace, and space. For NATO, multi-domain operations are 'the orchestration of military activities, across all domains and environments, synchronized with non-military activities, to enable the Alliance to deliver converging effects at the speed of relevance.' (Allied Command Transformation, 2022) Joint command structures enhance coordination among various armed services, whereas a multi-domain approach further incorporates military and non-military assets. This expanded integration is the primary distinction between joint and multi-domain operations. Apart from the expansion to include additional non-military actors and the collaboration of external stakeholders like private industries and institutions, one of the biggest challenges of multi-domain operations is integrating the new domains and synchronizing all military assets, especially in the background of new technologies, artificial intelligence, and improvement of command interoperability across all domains. (Allied Command Transformation, 2023) The multi-domain environment is highly complex and challenging, consisting of several domains, dimensions, layers, and factors. A better understanding of this gives a holistic view of the operational environment, which connects all these areas (see figure 1).

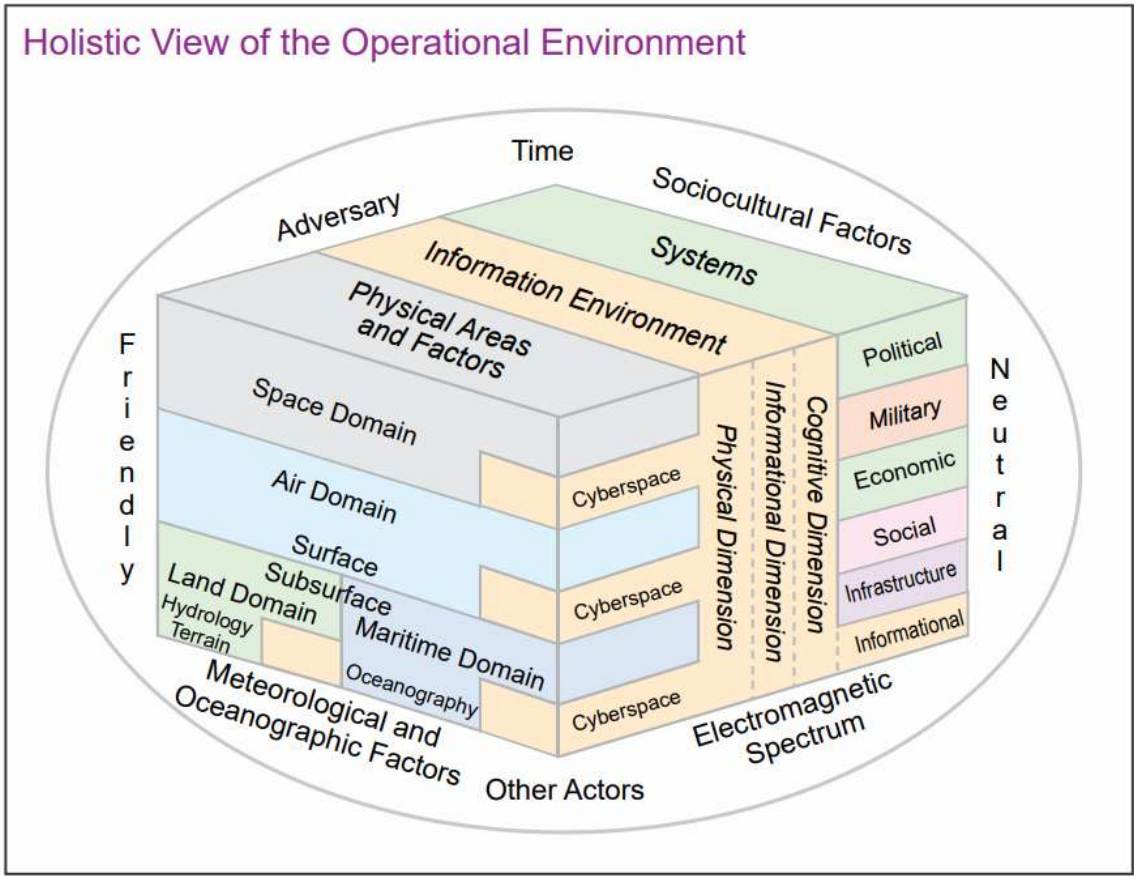

Figure 1: Holistic View of the Operational Environment based on source (JP 2-01.3, 2014)

The physical area encompasses the operational zones required for missions across the air, land, maritime, and space domains. These are connected to the information environment via the fifth domain, cyberspace. The information environment encompasses all individuals, organizations, and systems involved in gathering, processing, sharing, or acting upon information. It consists of three interconnected dimensions: physical, informational, and cognitive. The physical dimension is a material characteristic, capability, or both and tends to be natural or manufactured. The information dimension is the content, data, and processes individuals, groups, and information systems use to communicate. The cognitive dimension encompasses people and their interactions to understand information and events, make decisions, generate will, and act. The third important area comprises the six system factors that affect the operational environment and, therefore, need to be considered, such as political, military, economic, infrastructure, and informational factors. (JP 2-01.3, 2014) Military activities occur in all five domains and aim to achieve effects in the three dimensions, considering the six system factors.

Joint fire operates in all areas of the operational environment and plays a crucial role in this multi-domain battlefield. NATO defines joint fire support ‘as the coordinated and integrated employment of land-, air- and naval fire support platforms delivering indirect fires to achieve the required effects on ground targets to support Land Operations in the full spectrum of conflict.’ (NATO, 2015) That means fire support is a joint effort by armed forces using indirect systems for lethal and non-lethal purposes. It includes sensors and effectors of the Army, the Air Force, and the Navy, like unmanned and manned aircraft, naval surface fire support, artillery, mortars, or missiles, and cyber capabilities. (FM 3-09, 2024) It creates the conditions on the battlefield for operations, especially by ground-based forces. It is an essential component of multi-domain operations as it enables the integration of firepower from different military domains (air, land, sea, cyber, and space). Using synchronized attacks across various domains, joint fire can simultaneously weaken the enemy in multiple places, confuse them, and reduce their ability to fight back and achieve precise, synchronized effects on targets that align with strategic and operational objectives. In the physical dimension, artillery and missile systems engage targets on land or in the maritime domain, delivering kinetic effects to degrade enemy forces or infrastructure. In the informational dimension, joint fires depend on real-time intelligence and coordination, leveraging data processing to select, verify, and engage targets effectively. Cyberspace enables the collection of target intelligence and provides the framework for communication and coordination. Artillery fire missions can be guided using data from satellite reconnaissance or cyber-enabled targeting. In the cognitive dimension, joint fires shape enemy decision-making, erode morale, and influence its will by disrupting, degrading, or denying key assets or infrastructure.

While fire support is often seen as inherently joint, ground forces commanders may rely more on organic assets like field artillery for effective support. Fixed-wing aircraft availability depends on achieving air superiority and degrading enemy air defenses, while rotary-wing support also relies on these factors. Although naval gunfire support is advantageous, its availability is tied to the battle location. Therefore, ground commanders primarily depend on field artillery for fire support. (Saw, 2024)

‘The role of artillery is to destroy, neutralize, or suppress the enemy by cannon, rocket, and missile fire and to integrate and synchronize all fire support assets into operations.’ (FM 3-09, 2024) The core competencies of artillery are the coordination of fire support and the delivery of indirect fire. Achieving fire support requires the synchronization of C2, target assessment, and attack/delivery systems across all echelons of command. Effective fire delivery relies on the swift and continuous coordination of all components within the fire support system across every domain. The goal is to deliver the appropriate type and volume of fire precisely when and where needed to support the commander's operational plan. (FM 3-09, 2024) Effective planning, coordination, and synchronization of joint fire support are crucial to maximizing the use of all available assets to deliver lethal and non-lethal effects. (Golonka, 2021) One of the biggest challenges is deconflicting all of them in a multi-domain environment.

Tube Artillery vs. FPV-Drones

In a multi-domain approach, artillery, as a branch of the army, combines command, reconnaissance, and effectors in a system network. It is also given a special role as the leading provider of fire support. (von Dombrowski, 2024) The primary advantage of artillery lies in its high reliability, as it can operate around the clock, in all weather conditions, to target ground positions and deliver effects over large, deep areas. (NATO, 2015 pp. 2-1) Artillery can strike deep into enemy positions, shaping the operational area by isolating frontline forces from their support infrastructure, cutting off supplies and reinforcements, and continually degrading their capabilities. Where airpower used to do this job, the mission has moved to the hands of the guns and their increasingly precise means of deliverance. (Saw, 2024) Tube artillery is known for its quick response, precision, and ability to provide continuous fire support. It offers 360-degree coverage; the cannon can be aimed at any target within a complete circle around it, providing comprehensive targeting flexibility. Its wide range of ammunition, combined with advanced target acquisition systems, allows for the engagement of both specific and broad targets, with effects tailored to meet tactical needs. (NATO, 2015) This includes neutralizing enemy forces, such as their artillery, air defense systems, logistical supply facilities, and command structures. Fire support thus contributes to the firefighting of the land forces, achieves superior effectiveness, and reduces premature wear and tear of one's forces. (von Dombrowski, 2024) Where enemy air defenses or bad weather prevent the use of combat aircraft, armed drones, or attack helicopters, the army's fire support resources can work virtually around the clock, 365 days a year, if there are enough tubes and ammunition. (Geiger, 2023). Tube Artillery offers not only area but also precision fires. Modern ammunitions such as Excalibur, a 155-millimeter high-explosive artillery projectile designed for precision and extended range, equipped with an integrated global positioning system, inertial navigation guidance, and a unitary warhead, enables artillery operations in urban and confined areas, reducing the risk of collateral damage. (FM 3-09, 2024) However, the target acquisition system (using GPS) of precision ammunition is susceptible to the influence of enemy electronic warfare, which leads to a loss of the precision of the ammunition. (Zaluzhnyy, 2023) This technology is also much more expensive than unguided high-explosive ammunition. Mass fire from unguided grenades, therefore, still dominates the battlefield.

A significant disadvantage of artillery can be its complexity. Before a shot can be fired, an entire network must work together. It needs observers near the front who, in cooperation with the tactical commander of the combat troops, define targets, send them to the tactical operations center to decide, and then give the order to fire to the fire control center. This calculates the firing elements of the guns (barrel direction, barrel inclination, charge strength, and flight time of the projectile if it is to explode in the air) and passes these on to the guns. The time between reconnaissance of a target and combating can take several minutes. Modern guns, such as the PzH 2000, have a high degree of autonomy and can calculate their firing elements independently; support from a fire control center is no longer necessary.

Central to the modernization of Ukraine's artillery was the development of a ballistics calculator app compatible with Android devices that significantly improved the responsiveness and efficiency of existing artillery systems. Likened to "Uber for artillery," this software streamlines fire operations by providing a real-time situational picture and allowing forward observers to transmit target data over encrypted networks. These systems enable rapid target acquisition and engagement and ensure "every sensor, the best shooter" by simultaneously connecting observers, commanders, and fire units. (Nagl, et al., 2024 p. 101) However, this requires a change in the chain of command and clarifying how artillery fire is coordinated and prioritized.

Other limitations of using artillery include vulnerability to counter-artillery and electronic warfare. Electronic jamming devices can disrupt precision ammunition, entire fire control systems, and communication networks of tube artillery. This can disturb target acquisition and coordination between units, significantly impairing the ability to respond quickly to changing conditions. Electronic fire control and communications systems can be detected by enemy electronic surveillance, which can give away the position of the artillery. Especially after firing, the position of the tube artillery can quickly become a target for enemy fire, so it must be quickly repositioned. (Kagan, et al., 2024 p. 40) In the Russian-Ukrainian war, artillery plays a crucial role, accounting for 60-80 percent of the overall tasks, depending on the operational conditions and terrain. The success of military operations hinges on the effectiveness of artillery fire, making the "hunting" of enemy fire a primary focus for both sides. Consequently, counter-battery operations have become a key element of the armed conflict. (Zaluzhnyy, 2023)

The new players in multi-domain operations are commercial drones that provide indirect fire support. Like artillery, they combine command, reconnaissance, and effectors. The first deployment of modified "First Person View" (FPV) drones in the Ukraine war occurred in 2022. FPV drones are small unmanned aerial vehicles (UAVs) typically assembled from commercially available components, often adapted from racing drones. Initially, Ukrainian forces had limited resources, prompting soldiers to creatively repurpose commercial micro-drones (quadcopters) for reconnaissance and direct action. These drones, equipped with ammunition, were used to drop explosives onto Russian positions and vehicles. While using drones for such purposes wasn't a new concept, having been seen in previous conflicts, the innovation in Ukraine was the adaptation of racing drones for this task. Technical developments like miniaturization and enhanced performance of commercial drones improved their military capabilities. The significant improvement was the modification of these drones to carry warheads that could be flown directly to targets, providing more precision and effectiveness, especially against moving vehicles, like loitering munition tactics. (Geiger, 2024) FPV drones have key advantages over artillery in precision, agility, and stealth. They can be quickly and affordably deployed, serving as a low-cost option in some situations. Their small size and capability to fly at low altitudes help them avoid detection, making them very effective for hitting moving targets or suppressing enemy fire. Many tactical drones can be launched with minimal supporting infrastructure and operated from concealed, bomb-proof bunkers that are hard to detect. (Kagan, et al., 2024 p. 41) Additionally, these drones can provide real-time intelligence and strike targets without the logistical delays of traditional artillery, increasing their effectiveness in fast-paced combat situations.

In the war in Ukraine, the sound of drones has become so familiar to soldiers that their mere presence overhead is enough to force them to take cover. This psychological effect can "hold down" entire platoons, creating opportunities for one's forces to initiate an attack. This tactic mirrors the impact previously observed with indirect fire, such as artillery or mortars, which could suppress enemy movements and set the stage for offensive actions. This method of psychological warfare, through sound and fear, has proven effective in modern conflict, especially in Ukraine. (Geiger, 2024) On the other hand, the integration of tactical reconnaissance with attack drones, artillery, and attack rotary-wing aviation allowed the Russians to bring individual Ukrainian vehicles and infantry concentrations under precise fire throughout the depth of the tactical advance. (Kagan, et al., 2024 p. 27) Many reconnaissance drones have electro-optical, thermal, and infrared sensing capabilities to identify and strike targets day and night. The battlefield in Ukraine is almost transparent, with minimal cover. Numerous unmanned aerial vehicles provide effective reconnaissance and targeting capabilities at all times. These drones, including FPV attack quadcopters and fixed-wing strike drones, allow operators to accurately engage enemy positions and troops from several kilometers away, extending their range through relay drones. (Kagan, et al., 2024 p. 28) Both sides have begun implementing an integrated system connecting sensors, drones, and traditional artillery. Unmanned systems, primarily aerial, have become so common that they are now part of the anatomy of modern warfare. Their operators are fully integrating them into current operations. (Kagan, et al., 2024 p. 38)

However, like artillery, drones are not invulnerable and have their limitations. A critical challenge lies in their reliance on communication systems, which are susceptible to electronic warfare measures such as jamming, spoofing, or interference. Even drones designed for autonomous operation are not entirely immune to these disruptions. Moreover, electronic warfare isn't the only threat; drones are significantly impacted by adverse weather conditions, which can impair their functionality and operational reliability, a disadvantage not shared by traditional artillery shells. Unlike an artillery round's high-speed, difficult-to-detect trajectory, drones are relatively slow-moving and rely on electronic components, making them more vulnerable to detection and interception. Their electronic signatures can reveal their presence, enabling adversaries to target them through anti-aircraft measures or even electronic countermeasures. Furthermore, the payload capacity of tactical drones is limited, which restricts their ability to deliver broad-area effects. This limitation contrasts sharply with the massed firepower capability of tube artillery, which can saturate an area with fire. These challenges highlight the need for careful integration of drones into military operations, complementing rather than replacing traditional artillery systems to ensure robust and adaptive fire support capabilities in multi-domain operations. (Kagan, et al., 2024)

The following table (see figure 2) compares tactical drones with howitzers regarding various aspects, such as costs, capabilities, and logistics. To give concrete data, the research paper concentrates on the PzH 2000. Costs, ranges, and ammunition can vary compared to other howitzers. The field of drones is difficult to define, as their use is infinitely diverse and offers countless possibilities. For example, the ammunition a commercial drone is equipped with is only limited by its payload and the operator's imagination. Therefore, different examples have been selected for comparison.

Aspect	**Tactical Drones (FPV, quadcopter)**	**Howitzer (PzH 2000)**
Procurement costs	DJI FPV: 300 - 2000 €[6]	PzH 2000: 18 Mio €[7]
Ammunition costs	RPG-7 rocket: 100 – 500 $[8] Mines: 3 - 30 $[9]	The average price per artillery shell HE 3.500 $[10], Excalibur Guided Artillery Round 68,000$[11]
Supply chain	Easy production of commercial drones (UKR will produce 4 Mio per year[12])	Large supply chain for shells, fuzes, and propellant; traditional, established for decades

[6] (DJI, 2024)
[7] (Manthey, et al., 2023)
[8] (ANON, n.d.)
[9] (MacAlpine, 2024)
[10] (MacAlpine, 2024)
[11] (Freedberg Jr., 2016)
[12] (Saballa, 2024)

	small, modular supplies (batteries, cameras, payloads) and consumer-grade components can be locally sourced or 3D printed, small logistical effort: Drone + warhead = 3 kg[13] * 420 possible objectives = 1,26 t	Requires large quantities of heavy ammunition and high logistical effort: one combat load of 1 PzH 2000 = 60 shells (1 shell = 40 kg), per batterie with 8 guns = 420 possible obj. = 19 t
Maintenance and repair	Simple maintenance (replace rotors, batteries, or parts).	Mechanical systems require regular checks (gun barrel health), often in-field
Crew	Drone team: 3 - 5 (operator, analyst, technician (ammunition specialist), coordinator)	PzH2000: 3 - 5 (commander, driver, gunner, and two ammunition gunners)
Complexity	Low: Live images transmitted directly to a headset worn by the operator, often joint use of small teams consisting of reconnaissance drones and loitering munitions	High: System network of observers, combat troops, (fire control center), and several guns
Education	Basic training: 42-hour course, FPV combat use: 100-hour (15 days) course[14]	Commander: 6 months Gunner: 3 months
Range	Depending on the type of drone, FPV up to 15 – 20 km[15]	HE: 30 km, Rocket-assisted missiles with a range of up to 40 km, 54 km with a Velocity Enhanced Long-Range Artillery Projectile[16], VULCANO 155: up to 70 km
Combat load/Payload	grenades, anti-tank mines, mortars (up to 3 kg)[17]	60 shells (one 40 kg) 10 shots per minute
Precision	Depends on the capabilities of the operator, but high	Depends on ammunition: HE approximately 85% of all shells land within an area the size of a football pitch[18] VULCANO circular error probable (CEP) of less than 5 meters[19]

[13] (Zafra, et al., 2024)
[14] (Dronarium, 2024)
[15] (Gosselin-Malo, 2024)
[16] (Saw, 2024)
[17] (Hawser, 2024)
[18] (Rheinmetall, 2019)
[19] (Leonardo Electronics Division, 2021)

Mobility	Highly portable; often hand-launched; decentralized, highly flexible use in small units, easy to camouflage	Medium, self-propelled gun; depends on the ground and infrastructure (bridges), easy to clarify due to the size
Availability	fair-weather weapons, strong winds, rain, and low temperatures lead to significant performance losses	24/7, weather-independent
Protection	operators can launch drones from concealed or distant locations, often beyond the enemy's line of sight, minimizing exposure	protection for operators by maintaining a safe distance from the front line, "shoot and scoot" tactics to evade counter-attacks
Vulnerability	Vulnerable to electronic interference, shot down by air defense, 75% of losses due to friendly fire	Vulnerable to counter-battery fire and reconnaissance

Figure 2: Comparison of tactical drones and Howitzer PzH 2000 based on sources mentioned in the footnotes, table created by author

At first glance, drones seem to be a cheap alternative to howitzers. The cost of drones, especially FPV drones adapted for military purposes, can range from a few hundred to a few thousand dollars per unit. But, one must not forget that drones, such as loitering ammunition or kamikaze drones, are used in large quantities. Theoretically, these drones are cost-effective for precision strikes, especially against high-value or mobile targets. However, multiple drones are needed to make a hit depending on the operator's skills. According to a report of the Royal United Services Institute Ukraine is losing 10,000 drones per month in 2023. (Watling, et al., 2023) EW and friendly fire are the biggest factors. The number may have increased in the last year. The precise use of drones against high-value or mobile targets may still be more cost-effective than precision ammunition from artillery. However, when it comes to using explosive munitions and the high consumption of drones, the costs balance each other.

Built from off-the-shelf components, the production of FPV drones seems easy and cheap, but it is not without weaknesses. Ukraine is currently producing millions of drones for mass use. However, Ukraine is highly dependent on foreign suppliers. It cannot produce high-tech products such as chips and electric motors itself. For example, China controls 70 percent of the global drone market. Its export restrictions in December last year also affected Ukraine's ability to produce cheap drones domestically. (Porter, 2024) If this supply of supplies dries up, the entire production reaches a standstill.

Drones offer a lower logistical burden, requiring less infrastructure to deploy. While artillery systems can deliver massed firepower over extended periods, the operational costs increase with ammunition consumption and the need for logistical support, such as transporting and maintaining guns and shells. Tons of ammunition and a smooth supply chain are needed to keep an artillery battery running. The lifespan of howitzers is significantly longer than that of drones, but they also require regular maintenance, such as changing the barrel. During this time, they depend on special infrastructure and additional specialized personnel and are unavailable for combat.

Both systems require well-trained personnel. Training a complete howitzer crew takes several months. This is also because a howitzer is used in a system network, and all elements involved must be trained to ensure it functions smoothly. The training to become a drone operator only takes a few days or weeks. However, depending on the operator's talent, it also requires much experience to fly a drone precisely. Also, drone operators do not work in isolation. They are part of a team. One controls the drone using a remote controller and a headset that provides a live feed from the drone's camera. At the same time, another monitors a tablet displaying maps and offers navigational guidance or analysis of the data. Typically, a third soldier with a reconnaissance drone will have already identified the target. (Zafra, et al., 2024) In addition, some technicians assemble the drones on-site and equip them with ammunition.

Directing FPV drones to their targets results in a much higher accuracy than one would achieve with most artillery systems. This high level of precision allows drone operators to engage and destroy not just stationary but also moving vehicles that might otherwise achieve sanctuary from traditional artillery. However, drones still have far less explosive power than artillery, which can fire up to ten rounds of high explosives at a target within a minute. The artillery range is still greater, so it can cover much more than drones. Precision ammunition increases artillery accuracy but is also many times more expensive.

If you compare the mobility of both systems, FPV drones are ahead (see figure 2). They are very portable and can be carried by individuals. They can, therefore, also be used in a decentralized manner. As long as drones are not in use, they are easy to camouflage due to their small size, unlike howitzers. In principle, howitzers also have a high degree of mobility. They are off-road capable and can be used in almost any area. Even when not in use, they are easy to spot due to their size, so special attention must be paid to their camouflage.

The biggest advantage that howitzers have over drones is their reliability and availability. Regardless of visibility and weather conditions, howitzers can be effective under all circumstances. Their use is limited primarily by the supply of ammunition and fuel. However, its increased detectability makes it particularly vulnerable after use. Therefore, guns must immediately leave their position after each use to avoid counter-artillery fire. Due to their electronic signature, drones are easily detected using electronic warfare measures. The most effective means of halting drones has turned out to be electronic warfare systems. In the war in Ukraine, both sides utilize these systems to jam radio frequencies in targeted locations. However, the increasing use of FPV drones with optical fiber technologies on Ukrainian battlefields shows that countermeasures are also being sought here.

Conclusion and recommendations

The conflict in Ukraine highlights the critical role of tube artillery and FPV drones on modern battlefields and demonstrates current capabilities and future requirements. The future of both systems lies in the continued development of the technologies while integrating them with other systems and sensors to maximize their effectiveness in future multi-domain operations.

Future warfare demands a blend of precision and massed fires. Precision-guided munitions neutralize key targets, while high-volume fire restricts enemy movement, weakens formations, and prevents territorial gains. Ukraine's effective use of both demonstrates this balanced approach, targeting strategic assets with precision and overwhelming Russian forces with firepower. (Nagl, et al., 2024 p. 103)

While UAVs and loitering munitions offer distinct advantages in modern warfare, traditional artillery, particularly howitzers, retains a vital role. Artillery's capacity for massed firepower remains unmatched by current drone technology. The sheer volume of projectiles delivered by artillery creates a level of suppression and destruction that smaller drone platforms cannot replicate. This massed fire is crucial for weakening large enemy formations, disrupting their movements, and preventing them from gaining or holding territory during large-scale operations.

Furthermore, artillery's long-range engagement capability remains a significant advantage, particularly against entrenched positions or dispersed forces. While drones excel at targeting specific high-value assets with precision strikes, artillery is more effective at saturating larger areas with fire, creating a "suppressive effect" that hinders enemy operations. This area denial capability is crucial for supporting maneuver forces and shaping the battlefield. However, using precision-guided projectiles, such as the Excalibur round, which leverages GPS and inertial navigation systems to increase accuracy and reduce collateral damage, will allow tube artillery to be effective even in urban or confined spaces. The reduced need for mass fire saves ammunition and logistical resources, making artillery more efficient.

Artillery also plays a key role in multi-domain operations, integrating seamlessly with other fire support systems, such as air support and intelligence-gathering assets, to provide a comprehensive and coordinated approach to battlefield firepower. The future of artillery likely involves closer integration with advanced technologies, including UAVs and loitering munitions, creating a synergistic effect.

Drones will act as a force multiplier, complementing rather than replacing artillery. Small, readily available reconnaissance drones can provide persistent battlefield surveillance, identifying targets for both immediate FPV drone attacks and coordinated artillery strikes. This integration effectively brings the "reconnaissance-strike complex," traditionally an operational-level concept, down to the tactical level, enhancing the overall effectiveness of combined arms operations. (Kagan, et al., 2024 p. 40)

With drone spotting, mobile units such as tanks and infantry become more susceptible to artillery attacks, elevating the importance of artillery. Drone-assisted correction enhances the precision of artillery fire, making it even more effective. Furthermore, numerous mid-range reconnaissance drones now have laser designators, enabling even older towed artillery to execute precise strikes using laser-guided munitions. This represents a significant advancement in artillery effectiveness, particularly given the affordability of laser guidance and the improved accuracy over long ranges. Integrating UAVs and loitering munitions significantly enhances the efficacy of modern artillery systems. Drones provide real-time reconnaissance and targeting capabilities, offering an aerial perspective that complements ground-based fire support. By delivering accurate intelligence, UAVs enable artillery units to engage targets with greater precision and adaptability.

Modern artillery development focuses on enhancing mobility and survivability to address the evolving threats on the battlefield. Integrating self-propelled artillery systems with rapid deployment and shoot-and-scoot capabilities significantly improves mobility, allowing units to fire and relocate quickly, thereby reducing their exposure to counter-battery fire. Advanced systems like the PzH 2000 and the new RCH155 exemplify these innovations, combining firepower with agility.

To counter emerging threats such as electronic warfare, artillery units must adopt hardened communication systems and implement decentralized fire control mechanisms. These measures reduce the risks of network disruptions and ensure continuous operational capability even in contested electronic environments.

Furthermore, the network integration of artillery systems with sensors, drones, and ISR (Intelligence, Surveillance, and Reconnaissance) platforms is revolutionizing battlefield dynamics. This interconnected approach enables real-time "sensor-to-shooter" connectivity, allowing for faster target acquisition and dynamic fire adjustments. Tools like artillery fire-control software apps enhance coordination and accuracy, ensuring fire missions are executed precisely and efficiently.

Additionally, loitering munitions work seamlessly alongside artillery, addressing challenges that conventional firepower may struggle to overcome. These munitions are particularly effective for engaging high-value or hard-to-reach targets, providing precision strikes that minimize collateral damage. Together, UAVs and loitering munitions expand the tactical versatility of artillery, creating a dynamic and integrated approach to modern fire support operations.

As warfare evolves with the advent of digital technologies, artillery systems are not being replaced by drones but rather further adapted. The future of tube artillery lies in its integration with advanced systems, combining its unmatched firepower with the precision and flexibility of drones and loitering munitions. This synergy allows traditional artillery and modern technologies to coexist, providing superior fire support in multi-domain operations. Drones have significantly increased the effectiveness of artillery. With the integration of drones, artillery has evolved from the king of the battlefield to its emperor.

Bibliography

Allied Command Transformation. 2023. Allied Command Transformation leads the NATO Mulit-Domain Operations Conference. *Wellcome Allied Command Transformation.* [Online] September 11, 2023. [Cited: October 05, 2024.] https://www.act.nato.int/article/act-leads-mdo/.

—. 2022. Multi-Domain Operations: Enabling NATO to Out-pace and Out-think its Adversaries. *Welcome to Allied Command Transformation.* [Online] July 29, 2022. [Cited: October 05, 2024.] https://www.act.nato.int/article/multi-domain-operations-enabling-nato-to-out-pace-and-out-think-its-adversaries/.

ANON. n.d.. RPG-7D3 Russia Rocket-Propelled Grenade Launcher. *OE Data Integration Network.* [Online] n.d. [Cited: 9 December 2024.] https://odin.tradoc.army.mil/WEG/Asset/25caf13651021181e4e72e58d6e1e7f3#:~:text=Perhaps%20the%20primary%20reason%20RPG,and%20%24100%2D500%20per%20rocket.&text=Upgrade%20w%2Fbipod%20and%20improved,version%20since%20the%20late%201990s.&text=Folding%20varian.

DJI. 2024. Camera Drones. *DJI Store.* [Online] 2024. [Cited: 9 December 2024.] https://store.dji.com/ee/selection/camera-drones?from=site-nav&_gl=1*11w6mod*_up*MQ..*_ga*MTk4Njg4NDMwNC4xNzMxODQ2NjEw*_ga_HXRDE344GS*MTczMTg0NjYwOS4xLjEuMTczMTg0NjYyNC4wLjAuMA...

Dronarium. 2024. Dronarium Academy. *The first training center for drone pilots in Ukraine.* [Online] 2024. [Cited: 9 December 2024.] https://dronarium.academy/en/.

Edmonds, Jeffrey A. and Bendett, Samuel. 2023. *Russia's Use of Uncrewed Systems in Ukraine.* s.l. : CNA Corporation, 2023.

FM 3-09. 2024. Fire Support and Field Artillery Operations. *FM 3-09.* s.l. : Headquarters, Department of the Army, 2024.

Freedberg Jr., Sydney J. 2016. Excalibur Goes To Sea: Raytheon Smart Artillery Shoots Back. *Breaking Defense.* [Online] Breaking Media, 12 Januar 2016. [Cited: 15 March 2025.] https://breakingdefense.com/2016/01/excalibur-goes-to-sea-raytheon-smart-artillery-shoots-back/.

Geiger, Waldemar. 2024. Drohnen-Kriegsführung: Die Entwicklung der FPV-Drohnen im Ukrainekrieg. *Hartpunkt.de.* [Online] 11 January 2024. [Cited: 2024 November 17.] https://www.hartpunkt.de/drohnen-kriegsfuehrung-entwicklung-fpv-drohnen-ukrainekrieg/.

—. 2023. Mehr Rohre und mehr Reichweite – Die Zukunft der deutschen Artillerie. *Soldat und Technik.* [Online] Mittler Report Verlag GmbH, 14 August 2023. [Cited: 2 11 2024.] https://soldat-und-technik.de/2023/08/streitkraefte/35442/mehr-rohre-und-mehr-reichweite-die-zukunft-der-deutschen-artillerie/.

—. 2024. Tiefer Einblick in die zukünftige Artilleriestruktur der Bundeswehr. *Hartpunkt.de.* [Online] 6 June 2024. [Cited: 15 March 2025.] https://www.hartpunkt.de/tiefer-einblick-in-die-zukuenftige-artilleriestruktur-der-bundeswehr/.

Golonka, Adrian . 2021. The Role of Artillery in Joint Fire Support. *Safty and Defense.* 3, 2021, Vol. 7.

Gosselin-Malo, Elisabeth. 2024. Cheap first-person-view drones now hunting larger prey in Ukraine. *Defense News.* [Online] 8 August 2024. [Cited: 9 December 2024.] https://www.defensenews.com/global/europe/2024/08/08/cheap-first-person-view-drones-now-hunting-larger-prey-in-ukraine/.

Grey, Stephen, Shiffman, John and Martell, Allison. 2024. Years of miscalculations by U.S., NATO led to dire shell shortage in Ukraine. *Reuters.* [Online] 19 July 2024. [Cited: 16 October 2024.] https://www.reuters.com/investigates/special-report/ukraine-crisis-artillery/.

Hawser, Anita. 2024. Inside Ukraine's drone warfare: The rise of first-person view drones. *Defence Procurement International.* [Online] 18 July 2024. [Cited: 9 December 2024.] https://www.defenceprocurementinternational.com/features/maritime/ukraines-fpv-drones-fitted-with-grenades-and-anti-tank-mines-are-a-game-changer-on-the-battlefield#:~:text=They%20can%20carry%20payloads%20(grenades,%2C%20navigator%2C%20and%20drone%20opera.

JP 2-01.3. 2014. *Joint Intelligence preparation of the operational environment.* s.l. : Joint Chiefs of Staff, 2014.

Kagan, Frederick W., et al. 2024. *Ukraine and the problem of restoring maneuver in contemporary war.* Washington : Institute for the Study of War, 2024.

Leonardo Electronics Division. 2021. Vulcano 155 - Guided and unguided long-range 155 mm ammunition. *leonardo.com.* [Online] 2021. [Cited: 9 December 2024.] https://electronics.leonardo.com/documents/16277707/0/Vulcano+155+%28MM08723%29_HQ.pdf?t=1671440640166.

MacAlpine, Audrey. 2024. How Much Do Weapons Cost? From The Smallest Land Mine To The Largest Missile System. *United24Media.* [Online] 28 June 2024. [Cited: 9 December 2024.] https://united24media.com/war-in-ukraine/how-much-do-weapons-cost-from-the-smallest-land-mine-to-the-largest-missile-system-804.

Manthey, Florian and Vieth, Amina. 2023. Bundestag approves ten new self-propelled howitzers 2000. *Bundesministerium der Verteidigung.* [Online] 29 March 2023. [Cited: 9 December 2024.] https://www.bmvg.de/de/aktuelles/bundestag-genehmigt-zehn-neue-panzerhaubitzen-2000-5599760.

Nagl, John A. and Crombe, Katie. 2024. *A Call to Action: Lessons from Ukraine for the Future Force.* Carlisle Barracks, PA : US Army War College Press, 2024.

NATO. 2015. *AArtyP-5 NATO Fire Support Doctrine.* s.l. : NATO Standardization Office (NSO), 2015. Vol. Edition B Version 1 .

Porter, Tom. 2024. Business Insider. *China is limiting the sale of key components used to build Ukraine drones: report.* [Online] 10 December 2024. [Cited: 16 March 2025.] https://www.businessinsider.com/china-limiting-sale-parts-used-ukraine-drones-war-russia-report-2024-12.

Rheinmetall. 2019. Major Bundeswehr order. *Rheinmetall.* [Online] 8 April 2019. [Cited: 9 December 2024.] https://www.rheinmetall.com/en/media/news-watch/news/2019/2019-04-08_major-bundeswehr-order.

Saballa, Joe. 2024. Zelensky Says Ukraine Can Now Produce Four Million Drones a Year. *The Defense Post.* [Online] 3 October 2024. [Cited: 10 December 2024.] https://thedefensepost.com/2024/10/03/ukraine-produce-million-drones-2/.

Saw, David. 2024. The path ahead for tube and rocket artillery. *European Security and Defence.* [Online] 5 March 2024. [Cited: 8 December 2024.] https://euro-sd.com/2024/03/articles/36892/the-path-ahead-for-tube-and-rocket-artillery/.

Schnaubelt, Christopher M. 2023. Anyplace, anywhere, anytime. NATO and multi-domain operations. *Outlook.* 2023, Vol. 02.

UN OCHA. n.d. . Explosive weapons in populated areas. *UN OCHA.* [Online] United Nations Office for the Coordination of Humanitarian Affairs, n.d. . [Cited: 2 November 2024.] https://www.unocha.org/explosive-weapons-populated-areas.

United Nations. 2008. United Nation Treaty Collection. *Convention of Cluster Munitions.* [Online] 2008. [Cited: 2 November 2024.] https://treaties.un.org/Pages/ViewDetails.aspx?src=IND&mtdsg_no=XXVI-6&chapter=26&clang=_en.

von Dombrowski, Robert. 2024. Neue Aufgaben fuer die Artillerie. *cpmFORUM.* 2024, Vol. 6/23.

Watling, Jack and Reynolds , Nick . 2023. *Meatgrinder: Russian Tactics in the Second Year of Its Invasion of Ukraine.* s.l. : Royal United Services Institute for Defence and Security Studies, 2023.

Zafra, Mariano , et al. 2024. Combat in Ukraine is changing warfare. *Reuters.* [Online] 26 March 2024. [Cited: 15 December 2024.] https://www.reuters.com/graphics/UKRAINE-CRISIS/DRONES/dwpkeyjwkpm/.

Zaluzhnyy, Valeriy . 2023. Ukrainian Armed Forces Commander-in-Chief: Modern positional warfare and how to win it. *LB.ua.* [Online] 2 November 2023. [Cited: 7 December 2024.] https://en.lb.ua/news/2023/11/02/23656_ukrainian_armed_forces.html.

MAJ Fredrik Stadig. Sweden's NATO Membership and the Strategic Role of Estonia's Islands in Baltic Sea Security

Introduction

Over thousands of years, nature has shaped the geography around the Baltic Sea. This strategic inland sea, with connections to the global oceans, has shaped the military dynamics with its characterised short distances between coastlines, straits, islands, and inlets. Naval capabilities have been essential to exercise control over the Baltic Sea region, but the geographical landscape has also placed demands on the ability to conduct land warfare. The geostrategic importance of the Baltic Sea can be compared to other inland seas with limited inlets, such as the Mediterranean Sea through the Strait of Gibraltar or the Black Sea through the Bosphorus, where similar geographical conditions have influenced military operations and tactical efforts. In modern times, the air forces have also become equally vital in exercising power over the seas (Eliasson, o.a., 2021 s. 25).

Alliances are vital in modern warfare and change single nations' conditions and possibilities. Contributing to more significant opportunities for defence and reducing threats. Due to its geographical position, with the longest coastline in the Baltic Sea and extensive naval capabilities, Sweden's entry into the NATO alliance marks a shift in the defence of the Baltic Sea Region. The Baltic Sea with the islands of Estonia, Saaremaa and Hiiumaa, together with Denmark's Bornholm, Finland's Åland and Sweden's Gotland, play a crucial role in controlling the sea lines and airspace in the region (Sliwa, et al., 2022). Since Sweden's and Finland's accession to NATO, only one country bordering the Baltic Sea is not part of the alliance: Russia (Reinventing Mine Warfare in the Baltic Sea, 2024). Countries surrounding the Baltic Sea rely on the sea for their trade and prosperity; sea traffic in the Baltic Sea has increased throughout the years and is today a vital shipping web (Chief of Royal Swedish Navy, 2024) See Figure 1 (Maps on the web, 2022).

With its old naval traditions going back to the early 16th century, Sweden has stated that it will take a more proactive role in the Baltic Sea (Överbefälhavaren, 2024). With such a statement in mind, together with the topic, ‘Importance of the Estonian Islands in Defence of the Baltic Sea Region,’ this research paper explores the dynamic interplay between geography, military strategy, and international alliances in the Baltic Sea region, considerations of the enhanced defence posture resulting from Sweden’s NATO membership and its impact on the security of the Baltic states, including Estonia.

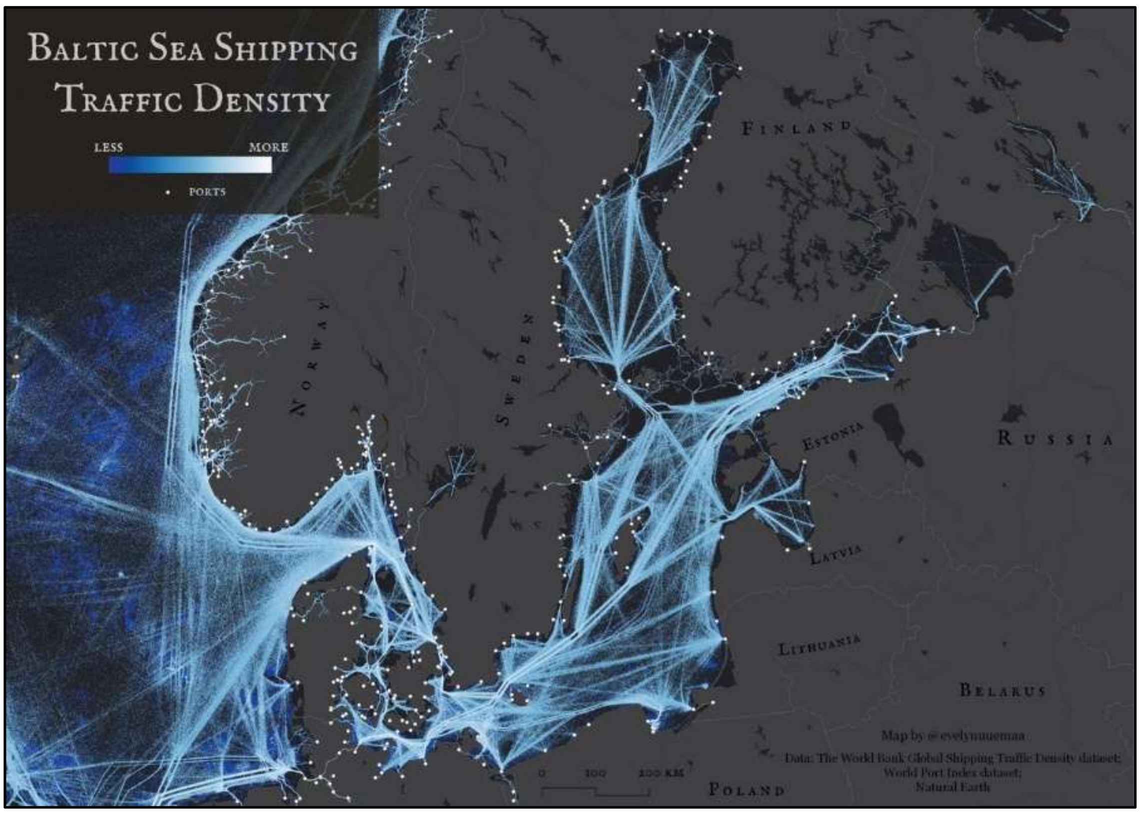

Figure 1: Baltic Sea Shipping Traffic Density. Source: (Maps on the web, 2022).

To explore the dynamic interplay between geography, military strategy, and international alliances in the Baltic Sea Region focusing on Sweden’s NATO integration and its effects on the strategic importance of the Estonian Islands, this research paper aims to answer the question: *How does Sweden’s integration into NATO enhance the strategic significance of the Estonian islands in the defence of the Baltic Sea?* The question considers the enhanced defence posture resulting from

Sweden's NATO membership and its impact on the security of the Baltic States, including Estonia.

The research paper will focus on three key aspects: Geostrategic locations, Military infrastructure and the role of Sweden as a new member of NATO. The geostrategic location makes the islands in the Baltic Sea Region a strategic position to monitor and control maritime traffic because the islands make them vital for surveillance and defence operations. The military infrastructure at the islands can contribute to facilitating and hosting military installations such as radar and missile defence systems and airbases that are mission-essential for NATO operations. When attributing Sweden's role as a new member, this gives another perspective to consider when discussing the defence of the Baltic Sea region, significantly since the importance of the islands.

I Estonian Islands in history: Why they matter

Throughout history, wars and conflicts have been fought where control over the sea and its surrounding areas have been a vital lifeline and have played a crucial role in the survival of the neighbouring countries in the Baltic Sea. Places of strategic importance in and around the Baltic Sea have been exposed to both occupation and threats of occupation, primarily by Russia. The Gulf of Finland has been particularly exposed from a historical Swedish and Russian perspective (Eliasson, et al., 2021 pp. 24-34).

The islands of Saaremaa and Hiiumaa on the west coast of Estonia have, due to their proximity to the Gulf of Finland, formed a strategically important outpost for the control of shipping, in and out of the Gulf of Finland in particular, as well as the surveillance of the Baltic Sea in general (Laanemets, 2021).

After Russia defeated the Swedes in the 18th century, plans were begun to strengthen the defence of the annexed Estonia's coastline since the conflicts with Sweden had demonstrated the lack of defence of strategic locations such as the sea route to Sankt Petersburg (Eliasson, et al., 2021 pp. 24-34). During the late 19th century, the foundation was laid for the Estonian coastal defence in the Gulf of Finland, which played an essential role during world wars and the Cold War (Treufeldt, 2009). By building systems of coastal defence batteries with artillery capabilities in combination with mines in critical chokepoints of the sea lines of communications (SLOCs), Russia controlled the sea routes to and out of Sankt Petersburg, securing its position of power. However, it turned out that the defence line was not as strong as Russia thought, and Sankt Petersburg would once again be threatened. When the German Empire launched one of the first primary joint operations towards the Russian-occupied Estonia, Operation Albion, during the First World War, they orchestrated an amphibious operation towards the Russian defence line of the Estonian Islands of Saaremaa and Hiiumaa. The effectiveness of the Albion operation outmanoeuvred the Russian defence. Despite a well-positioned coastal defence system with minefields in the narrow straits around the islands, with artillery batteries on well-chosen outposts and defence infrastructure to meet a counterattack from the sea, the Russians were outmanoeuvred by the German attack from the sea. The Germans gained an advanced posture and once again threatened the Russian mainland, especially the capital of Sankt Petersburg, ending the Russian occupation (Johanson, 2021 p. 302).After the German Empire's successful operation, Estonia announced its independence, which was gained and sealed on the 2nd of February 1920 with a peace treaty and borders. During the interwar period, Estonia took over the old coastal defence and invested millions of kroon (the former currency of Estonia) in rebuilding, restoring, and renewing the systems. At the same time, Estonia started cooperation with other nations to strengthen the defence of the surrounding area. One example is the cooperation that the Estonian Navy began in 1920 with Finland to establish a mine block line between the countries in the Gulf of Finland, see Figure 2 (Leskinen, 1999). This achievement created a locked-in effect for Russia's naval forces in Kronstadt, and once again, the threat towards Russia's heart, Sankt Petersburg, was imminent (Leskinen, 1999 pp. 18-19).

When the Soviets occupied Estonia during the Second World War, the Russians once again put much effort into the coastal defence of the region. The militarisation of the Estonian islands became vital for the Soviet defence of the Baltics, utilising the islands as an outpost for observation and surveillance of the sea routes in the Baltic Sea (Keep out! No entry! Exploring the Soviet military, 2019).

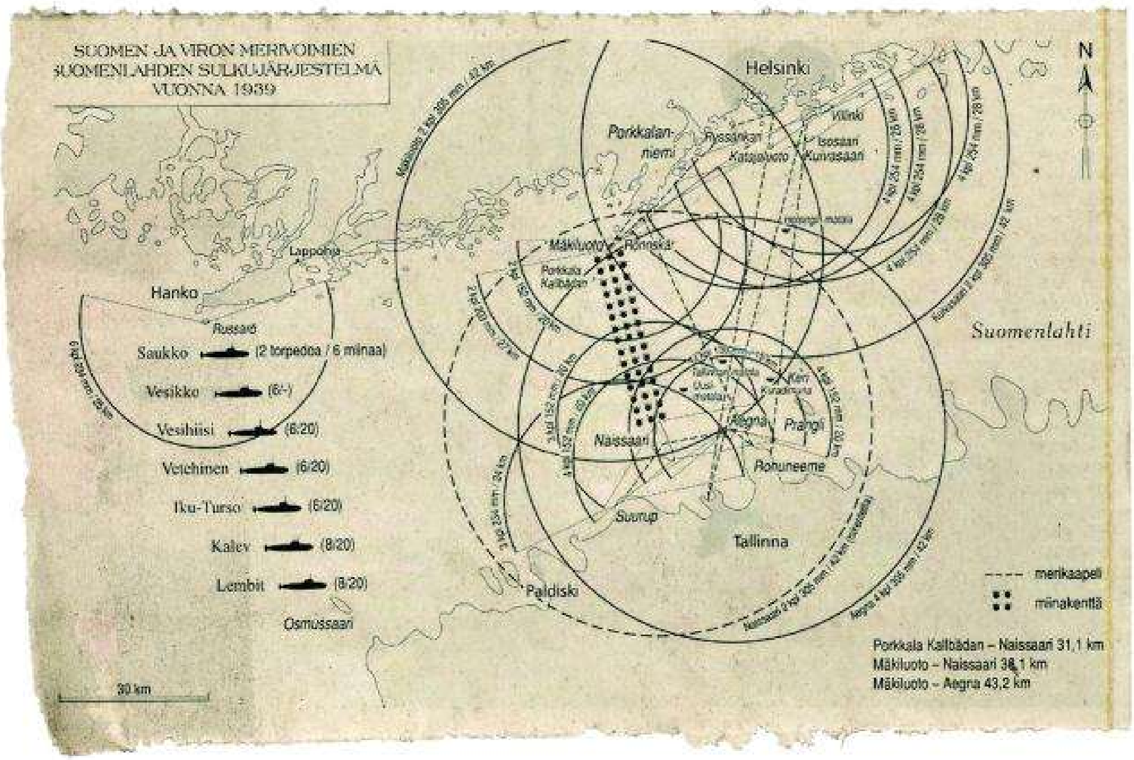

Figure 2: The Gulf of Finland Lock in 1939. Source: (Leskinen, 1999).

II Why the Estonian Islands are essential for defence today

The Estonian islands continue to be strategically important terrain for the defence of the Baltic Sea region. Despite the historical perspective of a noticeable military presence, the islands today are nearly demilitarised in comparison. The manning of the coastal batteries and the extensive minefields in the shallow straits are now in the past, and the defence is dependent on the all-volunteer Kaitseliit, the Estonian Defence League (EDL) (Kaitseliit, 2024). Through the continuous development currently taking place in the territorial defence of Estonia, where the EDL utilises local advantages, leadership, and coordination between and within the various regions, it has dramatically improved in recent years (Kaitseliidu peastaap, 2024).

Several exercises have been conducted with Saaremaa and Hiiumaa as their scenery over the past couple of years to show the importance and defence of the Estonian islands (Estonian Defence Forces, 2024). The main focus of these exercises is to ensure the military presence at the islands, which is vital for the entire armed forces, especially for the Estonian Navy and its Special Forces, to improve their operational capabilities. Exercises focusing on unconventional warfare, special reconnaissance, and direct-action missions increase readiness and interoperability with NATO allies while underlining Estonia's ability to maintain a robust military force that can respond to various security challenges (Joint Forces, 2024).

Even if the islands are not fully militarised to the extent of the past, the exercises display that it is imminent to keep a military presence on the islands. Another way to enhance the military effort without massive militarisation is to increase surveillance at strategic locations, such as Saaremaa and Hiiumaa. By using this strategic advantage of the islands and ensuring surveillance of the Baltic Sea, the Estonian government have decided to enhance the infrastructure at the islands, leading to better overall situational awareness. This improved infrastructure has been building up for a couple of years. It is still a significant priority for the armed forces to acquire new surveillance systems, offering the advantage of covering air and naval traffic (Estonian Defence Forces, 2022).

III Sweden's NATO membership: What it means for the Baltic Sea

Due to Russia's full-scale invasion of Ukraine, the Swedish posture and policy of neutrality were changed after almost 200 years. From a historical point of view, Sweden's main adversary has always been Russia, and ever since the French Fieldmarshal Jean Baptiste Bernadotte left the Napoleonic war and became the king of Sweden, better known as Charles XIV John, the policy of neutrality was stated for the Swedes in 1812 (Billström, 2024). Sweden's posture of non-alignment in peace and neutrality in war was essential to the region's stability throughout the Cold War era. The Swedish well-built and fully developed concept of total defence and Sweden's broad defence industry helped Sweden's role as one of the dependent diplomatic countries during the Cold War (Fedina, o.a., 2024). With the Cold War ending, there were new hopes for everlasting peace. A total downsizing of the Swedish Total

Defence concept and a significant downsizing of the Swedish Armed Forces (SwAF) started, and the shift of Swedish neutrality started. Coming from a time of domestic politics where military alliances were taboo, Sweden entered the NATO initiative Partnership for Peace in the mid-1990s. The SwAF focused on crisis management in a NATO context in the Balkans, with the start of implementing some of the NATO standards to make them more interoperable (Brommesson, et al., 2022).

With increasing peace enforcement engagement in the Global war on terror, the SwAF kept its mandatory conscript service on hold, focusing on all-employed Armed Forces. Due to the Russian invasion of Georgia in 2008, the Swedish defence posture was transformed and discussed, and voices rosed to increase defence spending (Brommesson, et al., 2022). With the annexation of Crimea in 2014, together with Russia's intense border crossings of Swedish airspace, questions were raised among politicians together with the Supreme Commander that the Swedish defence posture must change, and conscript service must reintroduce a compulsory military service together with all employed (Brommesson, et al., 2022).

Seeking bi, tri and multilateral security agreements with the closest partner nations and neighbouring nations, such as the Nordic countries with emphasis on Finland, the United Kingdom, and the USA, to guarantee the security of Swedish sovereignty became an assurance for and a start of deeper international cooperation. Although security guarantees had been given to Sweden earlier in history, the official posture was changed and unlocked. Since World War I, Finland has been one of the closest allies to Sweden due to its shared history and support during harsh times and its belief in robust diplomatic neutrality and total defence posture (Brommesson, et al., 2022).

With the Russian war in Ukraine and the Russian narrative of ultimatum and threats demanding a change of European Security, Sweden, together with Finland, left their posture of non-alignment and neutrality and applied to be a member of a defence alliance, NATO (Billström, 2024). As Russia's continuous aggressions towards Ukraine and alignment with Belarus have become an imminent threat to Sweden and its neighbouring countries of the Baltic Sea, especially Poland and the Baltic States, Sweden had to make a change in its defence posture to counter this security threat (Regeringen, 2022).

IV Deterrence and security in the Baltic Region

To further investigate the implications for regional security, it is crucial to understand what deterrence is and how it applies. Straightforwardly, deterrence could be explained through the lens of the American political scientist Michael J. Mazarr as all the active measures one state or actor takes to prevent another state or actor from using force on a state. Furthermore, deterrence can be divided and used by denial or punishment. To implement deterrence by denial, a state or actor must use much force to reduce the risk or make it difficult (deny) for an aggressor to succeed. As for deterrence by punishment, it simply means that a state or actor as a potential aggressor is punished if it proposes any form of force against another state or actor (Mazarr, 2018). Both strategies require credible threats and the perception that the costs of aggression balance any potential benefits, which are essential to maintaining peace and security in the region. Additionally, the effectiveness of deterrence relies on the aggressor's assessment of the determination and capability of the deterrent force, further highlighting the importance of strong alliances like NATO (Mazarr, 2018).

One of the biggest concerns regarding the overall security of the Baltic Sea Region is Russia's imminent threat and its extensive anti-access aerial denial (A2AD) capability. The Russian A2AD capability is a development of the former Soviet air defence doctrine initially developed in Poland and East Germany to defend Warsaw Pact forces from Western air power. Integrated, overlapping radars and multiple missile systems provide extensive coverage in depth and altitude, creating a large and almost impenetrable air defence bubble. Russia has developed the concept further and uses modern and potent systems. Similar capabilities as Russia exist in other countries; Western systems are referred to as integrated air defence systems (IADS) or integrated air and missile defence systems (IAMD) (Dalsjö, o.a., 2020).

If A2AD capabilities are the most imminent threats, the most realistic is Hybrid attacks. To further describe hybrid warfare, there is an urge to define its profound meaning. Though there are many different opinions of what Hybrid warfare is, Frank G Hoffman's definition is well articulated, stating that it '[…] incorporate a range of different modes of warfare including conventional capabilities, irregular tactics and formations, terrorist acts including indiscriminate violence and coercion, and criminal disorder.' (Hoffman, 2007).

One way for NATO to exercise deterrence against Russia is to conduct extensive exercises. To increase NATO's ability to rapidly reinforce its allies, the largest NATO exercise in decades, Steadfast Defender, was conducted in 2024. Within the framework of Steadfast Defender, the annual Estonian Defence Forces Exercise Spring Storm was performed, with a clear focus on the strategically important islands of Saaremaa and Hiiumaa. The exercise tested the readiness of the units within the framework of a defensive operation. At the same time, Estonian territorial forces cooperated with allies to improve interoperability between the allies (Republic of Estonia Defence Forces, 2024).

In 2024, the annual exercise Baltic Operations (BALTOPS) was part of NATO's extensive exercise series. BALTOPS, one of NATO's oldest maritime exercises, started in 1971 with exclusive participation from NATO countries but has developed over the years. In 1993, the exercise also opened to partner countries (NATO, 2017). 2024 marked the year of the largest BALTOPS since its start, with all participating countries being NATO members due to Sweden's recent accession. NATO's newest member played a key role in the exercise, demonstrating Sweden's unique expertise in amphibious operations in the complex environment of the Stockholm archipelago. Swedish amphibious units contributed with high mobility and precision with their advanced capabilities of a coastal combat operation in archipelago terrain. The realistic dimension of the exercise gave a clue of how capable Sweden and NATO are in strengthening regional security and stability with a scenario that easily could be applied to the Estonian Islands (Försvarsmakten, 2024).

BALTOPS 2024 showed that NATO strives to continue its deterrence and defence posture according to its core tasks, with enhanced collective readiness and interoperability. Aside from bringing new capabilities to the alliance, Sweden brings vital ground for launching regional operations. To handle the alliance's collective readiness, NATO countries must uphold a robust and well-functioning Host Nation Support (HNS) (NATO, 2022 p. 6). One of the essential and main components during the BALTOPS was the establishment of a Forward Logistics Site (FLS). As a part of an overall NATO logistic concept, this maritime logistics hub ensured that units could quickly and efficiently receive supplies and support required to maintain operational endurance. Their participation as a full NATO member improved interoperability with other allied forces and sent a strong signal of cohesion and readiness to address potential threats in the Baltic Sea region jointly (Försvarsmakten, 2024).

In November 2024, the prime ministers of the Nordic-Baltic Cooperation came together for the Nordic-Baltic summit in Sweden. The outcome of the meeting between the countries in the Baltic Sea Region was a clear stance against Russia's continued aggressive posture in the region, Russia's war in Ukraine and how the countries should continue cooperating for a more stable and secure existence in the Euro-Atlantic region (Government Offices of Sweden, 2024). The unique thing about the meeting was that all countries are now also part of NATO, which also sends a signal to Russia in a unified message. The apparent cooperation between the countries demonstrates the importance of the collective approach and the deepened cooperation that prevails between the countries.

Both NATO's exercise activities in the Baltic Sea region and the increased cooperation between the Nordic countries and the countries in the region create the conditions for a stance that eventually benefits the Baltics and Estonia. By extending the geographical depth that Sweden offers, both with the port of Gothenburg on the west coast, ports on the east coast and not least Gotland, the conditions for an active stance in deterrence towards Russia increased (Wills, 2024).

V Defence strategies in the Baltic Sea Region: The Estonian perspective

The concept of a defence strategy originated from Liddell Hart's Grand strategy theories, which were later developed by Colin Gray. With roots in these theories, some nations have developed their own and, in some perspective, more comprehensive strategies called security strategies. Central elements to measure how realistic a state's security strategy is are ends, ways, and means, where ways should be viewed as the core of the strategy and ensure criteria for success for state security interests. The Swedish scholar Jacob Westberg has analysed the concept of security strategy and believes that other elements within the strategy approach influence a state's choice of security strategy. For example, by adding the element of environment to a state strategy, geographical aspects can be addressed in a structured way. Within the framework of this development, countries such as Finland and Sweden have come to develop their national security strategies (Westberg, 2023 pp. 25-30).

Within the strategy framework, states seek different approaches to have as coherent and comprehensive a strategy as possible and why states seek bi, tri and multilateral agreements with other states.

Unlike Sweden, Estonia has been a member of NATO’s collective defence since 2004. When looking into the NATO alliance, it is essential to know what was stated in the treaty by its founding members in 1949. The two cornerstones of the NATO treaty are Articles 3 and 5. Article 3 emphasises the need for members to develop and maintain their resilience and individual defence capabilities, while Article 5 is most often emphasised when NATO is mentioned. Article 5 states the principle of collective defence, where an armed attack on one member is considered an attack on all. However, it is crucial for NATO that each country commits to strengthening its political, economic, and military preparedness to resist threats and strengthen the alliance (NATO, 2025). NATO’s core tasks are described in the NATO Strategic Concept launched at the NATO Summit in Madrid in 2022. Through deterrence and defence, crisis prevention and management, and collective security, NATO ensures peace and stability in the Euro-Atlantic region (NATO, 2022). Like Estonia, Sweden is now bound to protect member states through political consultation and military defence.

NATO’s Strategic Concept shows the way for NATO’s perspective towards Russia. By declaring that it intends to defend every inch of its allies’ territories, NATO has shown that it takes the threats to the existing international order seriously and is also prepared to protect it at all costs. Within the framework of the 360-degree defence that NATO expresses in its concept, the use of capabilities in its maritime domain is one of the cores of the active defence of chokepoints. (NATO, 2022). Although it is not expressed, some of these chokepoints are strategically located, like the Estonian islands.

Within the framework of NATO's 360-degree defence, there has been a need to reinforce NATO's eastern flank with troops, the so-called Forward Land Forces (FLF). At the same time, defence preparations expanded with a comprehensive review of the Alliance's joint regional defence plans over the Alliance's area of interest. With both Sweden and Finland as new members of the alliance, NATO's opportunities have been strengthened regarding new capabilities and the use of both countries' long experience in defending the Baltic Sea (Wills, 2024).

Another multilateral agreement of interest within the defence strategy is the defence cooperation Joint Expeditionary Force (JEF), which, unlike NATO, is not an alliance. The JEF cooperation was formed in 2014 to improve security in Northern Europe and focuses on complementing NATO operations and strengthening regional defence and security through interoperability and joint training. The United Kingdom is the framework nation, and Estonia and Sweden are part of this security cooperation (JEF, 2025). Unlike NATO, the countries within JEF do not need consensus on decisions and, therefore, can act more rapidly when the situation is deteriorating.

The long tradition of close ties between Estonia and Sweden has been formalised in different bilateral defence agreements covering several topics, such as procurement, exchange of information on sea surveillance and cyber security. Sweden's donations of weaponry to the Estonian Defence Force is a showcase of mutual trust and understanding of the security environment of the Baltic Sea Region (Estonian Ministry of Defence, 2011).

Discussion

As discussed above, the Baltic Sea's SLOCs are essential for trading and the region's economic prosperity. With this, Russia, its ports in Sankt Petersburg and Kaliningrad, are as dependent on the sea routes in the Baltic Sea as the ports in Sweden, Finland, Estonia, Latvia, Lithuania, Poland, and Germany (Chief of Royal Swedish Navy, 2024 p. 35). Due to the geographical location of the Estonian islands Saaremaa and Hiiumaa, these islands prolong the geographical depth to the mainland of Estonia, creating a natural buffer zone to an already strained depth to Russia, making the islands still as crucial for the defence, not only for Estonia but for the entire region.

Estonia’s recent increase in investments in mines, missiles, surveillance systems, and surveillance infrastructure in the islands is one good example of how proactive actions could benefit the entire region. By using strategic parts of the geography in the Baltic Sea, there is a possibility to extend the length of the surveillance system, which would make the covering picture better, denser and more comprehensive with the synergies of a notable increased early warning for any incoming threat.

Estonia’s longstanding bilateral agreements and involvement in sea surveillance with its neighbouring countries in the region is the Sea Surveillance Cooperation Baltic Sea (SUCBAS). SUCBAS is a fundamental framework for maritime surveillance, information exchange and operational cooperation in the Baltic Sea Region, currently led by the navies of Finland, Sweden, Denmark, Germany, Estonia, Latvia, Lithuania, Poland and the United Kingdom. By facilitating the exchange of maritime data traffic, information and expertise between the countries in the Baltic Sea, SUCBAS contributes to an increased understanding of activities in the region. Through increased cooperation between the national structures of the different states, such as security, maritime surveillance, environmental protection, and law enforcement, SUCBAS allows the participating countries to share information with relevant national government agencies. This ensures that civilian and military stakeholders benefit from and improve cooperation and intelligence sharing, which creates an increased Maritime Situational Awareness (MSA) (European Cooperation on Coast Guard Functions). This cooperation is of paramount importance for the MSA of the Baltic Sea in the short term and for the defence of the Baltic Sea Region in the long term. Thus, these systems and the interconnectivity from other countries like Sweden benefit the overall early warning systems when interconnected (Sliwa, et al., 2022).

While it is favourable to invest in surveillance, as mentioned earlier on the islands in Estonia, the vulnerability of such systems also increases, making the value of absolute protection relevant. One way to mitigate such risk is the JEF cooperation, which could be viewed as a gap filler between national defence plans, Swedish and Estonian, and NATO’s regional plans. Such a gap filler is efficient when the time is of the essence for responding. When the recent escalation of attacks towards critical underwater infrastructure increased, the first responder into the Baltic Sea was not NATO; it was JEF (GOV.UK, 2025).

However, reestablishing batteries and crews, as in World War II or the Cold War, may not be relevant; thus, such fortresses belong to the past. Nevertheless, it can still be considered crucial to have a continuous military presence stationed on the islands to avoid ending up in a situation like Crimea in 2014, when ‘green men’ showed up in Ukraine, and Russia denying its un-involvement in its classical manner. Many of the exercises conducted on the islands have demonstrated such hybrid scenarios in Estonia and Sweden. With less military presence on the islands, they are still vulnerable to hybrid operations and pre-emptive strikes, both kinetic and non-kinetic, such as cyber-attacks and information operations, because of their proximity to Russian military installations in Sankt Petersburg and Kaliningrad (Pawlak, 2024). To be better to counter hybrid threats on islands is to do as Sweden has done with Gotland and once again place continuous troops over time and not just only during exercise.

Another way to mitigate the gaps between the nation’s defence plans and NATO’s regional plans has been to integrate the islands into the overall defence of the Baltic Sea Region. This was previously not possible when Sweden and Finland were not members. However, it has now changed as Sweden’s Gotland has shown that it is crucial for the regional defence of the Baltic Sea Region and, thus, Estonia (Dahlberg, 2022).

Many military strategists describe Gotland as an unsinkable aircraft carrier, clearly showing how important the island is to Sweden and the entire region. However, just looking at a map of the Baltic Sea will point out that Saaremaa is almost as big as Gotland. The fact that NATO has gained Sweden as a member provides the conditions for an additional layer in defending the Baltic Sea, so militarising the Estonian Islands will also add another layer. The islands of Bornholm, Saaremaa, and Hiiumaa, together with Gotland, provide opportunities for NATO to be an active deterrent in the Baltic Sea region (Lucas, et al., 2022).

If Russia were allowed to move its A2AD capability to any of the islands in the Baltic Sea, this would affect the entire Baltic Sea Region and Europe. As the Russian A2AD capability has a very high deterrent effect due to its large number of conventional forces in the region, a concern that has made NATO strengthen its eastern flank, some defence studies have shown that the Russian “bubble” could be overrated. Although war is unpredictable, the actions of NATO, the enhanced European capabilities, and strong support from the US, NATO, and its allies could effectively counter Russia in the Baltic Sea Region (Dalsjö, et al., 2020).

NATO’s FLF, with its enhanced missile defence (IAMD), is one vital part of NATO's capabilities in Estonia. Furthermore, Estonia has also acquired air defence systems to increase deterrence against Russia. Joint exercises have been an essential part of testing these systems, and they play a significant role in strategically central locations such as Saaremaa or Hiiumaa.

However, if NATO’s deterrence towards Russia increases, NATO needs to balance its stance so as not to destabilise the region. A military escalation by NATO, or a sharp increase in the military presence of the islands, could send the wrong signals to Russia, which in turn could be viewed as an escalation and thus also lead to an increased Russian military presence in the immediate area (Sliwa, et al., 2022).

In late autumn 2024, some cuts to the critical underwater infrastructure occurred in the Baltic Sea. Cutting cables between countries such as Sweden, Finland, Estonia, Lithuania, and Germany have demonstrated vulnerability in the vicinity of the Baltic Region. Ships that assert to have accidentally let their anchor drag on the bottom for several kilometres and thus demonstrated questionable seamanship are a method used by the ships investigated by coastal states. Depending on how the various investigations proceed, more and more information about the cable cuts will be discovered, and clarity will be presented. Until then, there will be speculation about which actor, state or not, is behind it. Some experts claim that a Russian response to the increased NATO activity is happening in the Baltic Sea. With the swift actions taken by both Finnish and Swedish naval forces, NATO and the surrounding states in the Baltic Sea have shown that any disruption, intentionally or not, is met by actions and has to be investigated. Whether these actions would have been taken if Sweden and Finland had not been a part of NATO is questionable.

Over the years, a series of realistic exercises in Estonia have demonstrated the possibility of quickly facilitating NATO forces. The islands have been mainly used as logistics hubs for continued operations under such conditions (A Brief Naval Overview of the Baltic Sea Region, 2024). Although the Estonian government is investing in the islands, the general level of the military infrastructure is substandard and outdated. There are currently limited possibilities and capacity to facilitate a more prolonged NATO operation on the islands (Veebel, et al., 2019).

Due to Sweden's accession to NATO and the deepening cooperation within the alliance, the security dynamics in the Baltic Sea Region are continuously transforming. For Estonia, this means new opportunities to strengthen its defence and deterrence capabilities while geographical and strategic factors, such as the importance of islands, come into focus. This emphasises the importance of regional coordination in mitigating these security challenges (Westberg, 2023 pp. 55-57). This shows that Sweden's membership creates new conditions for a more coherent defence strategy in the Baltic Sea, affecting Estonia's strategic priorities (Claesson, et al., 2021 p. 184).

Conclusion and implications

This research paper suggests that the geography of the Baltic Sea has not changed, and short distances between the countries have remained the same. In this context, the defence and the military presence remain essential but with different capabilities. The security guarantees to protect itself and its territory are crucial, not least emphasised in Article 3 of the NATO Charter. Sweden's NATO accession has meant a lot for the Alliance's defence strategy in the Baltic Sea, with a clear connection between the islands, especially the Estonian ones. A nation's advanced military capabilities, together with a country's developed military infrastructure and geostrategic position, could strengthen NATO's operational readiness in the immediate area.

Due to the proximity to Russia and the absence of a military presence, the vulnerability of the Estonian islands increases the threat of hybrid operations, which both Estonia and NATO need to manage actively. With Estonia's long-term plan for both the development of the military infrastructure and the acquisition of equipment to defend the islands, countries in the vicinity will need to support them to ensure complete security. A security system is built by actively conducting exercises and constantly developing and exploring new capabilities. The outcome is a better defence that is more sustainable and adapted to all threats. A feasible path is, therefore, for Sweden and Estonia to improve interoperability between the countries, especially in the maritime domain, which could be crucial for maximising the security benefits of Sweden's NATO integration. However, the subject can be further developed and broadened into more areas, including all countries within the Alliance, to ensure that NATO remains an essential component of the defence of Europe in general and the Baltic Sea in particular.

References

A Brief Naval Overview of the Baltic Sea Region. **Savitz, Scott and Winston, Isabelle. 2024.** s.l. : RAND Corperation , 2024.

Are Current Russian Expeditionary Capabilities Capable of a Coup de Main in Sweden? **Freeman, Suzanne. 2021.** s.l. : Center for Strategic and International Studies, 2021.

Balti laevastiku Läänemere rajooni rannakaitse. 2023. Balti laevastiku Läänemere rajooni rannakaitse. *Vikipeedia.* [Online] 13 September 2023. [Cited: 30 December 2025.] https://et.wikipedia.org/wiki/Balti_laevastiku_L%C3%A4%C3%A4nemere_rajooni_rannakaitse.

Billström, Tobias. 2024. Ministry for Foreign Affairs. *https://www.government.se.* [Online] Government Offices of Sweden, 20 March 2024. [Cited: 28 November 2024.] https://www.government.se/speeches/2024/03/statement-of-government-policy-following-swedens-accession-to-nato/.

Brommesson, Douglas, Ekengren, Ann-Marie and Michalski, Anna. 2022. Sweden's Policy of Neutrality; Success Through Flexibility? [book auth.] Caroline de la Porte, et al. *Successful Public Policy in the Nordic Countries: Cases, Lessons, Challenges.* Oxford : Oxford University Press, 2022.

Chief of Royal Swedish Navy. 2024. *Speed M - Proceed at Maximum Speed.* Stockholm : SwAF, FMLOG, Grafisk Produktion, 2024.

Claesson, Michael and Carlander, Zebulon. 2021. *Vägval - Framtiden för Svensk säkerhet.* Stockholm : Ekerlinds förlag, 2021.

Dahlberg, Yasmine . 2022. Europe. *https://www.cpreview.org/.* [Online] Columbia Political Review, 12 May 2022. [Cited: 28 November 2024.] https://www.cpreview.org/articles/2022/5/sweden-and-nato-from-neutrality-to-reality.

Dalsjö, Robert and Jonsson, Michael. 2020. *Beyond Bursting Bubbles - Understanding the Full Spectrum of the Russian A2/AD Threat and Identifying Strategies for Counteraction.* Stockholm : Swedish Defence Research Institute, 2020. FOI-R-4991-SE.

Deterrence in the Nordic-Baltic Region: The Role of the Nordic Countries Together With the U.S. Army. **Pyykönen, Juha and Forss, Stefan. 2019.** s.l. : US Army War College, 2019.

Eesti merekindlused. 2021. Eesti merekindlused. *Vikipeedia.* [Online] Vikipeedia, 21 December 2021. [Cited: 30 December 2024.] https://et.wikipedia.org/wiki/Eesti_merekindlused.

Eliasson, Per and Ericson Wolke, Lars. 2021. *Mellan Neva och Nordsjön - Förutsättningar för att genomföra väpnad strid i Östersjöområdet.* Lund : Nordic Academic Press, 2021.

Estonian Defence Forces. 2022. *Estonian Defence Forces Annual Report.* s.l. : Strategic Communication Department, General Staff, Estonian Defense Forces, 2022.

—. 2024. News. *Estonian Defence Forces.* [Online] 7 December 2024. [Cited: 28 February 2025.] https://mil.ee/en/news/estonian-defence-league-and-allied-units-conducted-simulated-battles-near-sirgala/.

Estonian Ministry of Defence. 2011. Estonia and Sweden concluded a defence cooperation... *Republic of Estonia Ministry of Defence.* [Online] 7 February 2011. [Cited: 25 January 2025.] https://kaitseministeerium.ee/en/news/estonia-and-sweden-concluded-defence-cooperation-agreement.

European Cooperation on Coast Guard Functions. Sea Surveillance Cooperation Baltic Sea (SUCBAS). *European Cooperation on Coast Guard Functions.* [Online] [Cited: 02 February 2025.] https://coastguard.europa.eu/node/469.

Fedina, Katja and Black, James. 2024. Research & Commentary. *https://www.rand.org/.* [Online] RAND, 22 March 2024. [Cited: 28 November 2024.] https://www.rand.org/pubs/commentary/2024/03/what-swedens-accession-means-for-nato.html.

Försvarsdepartementet. 2024. *Totalförsvaret 2025–2030.* Stockholm : Regeringens proposition, 2024.

Försvarsmakten. 2024. Aktuellt. *Amfibiekåren i spetsen för Baltops 24.* [Online] 20 June 2024. [Cited: 29 December 2024.] Amfibiekåren i spetsen för Baltops 24 - Försvarsmakten.

GOV.UK. 2025. Armed Forces. *Defence and armed forces.* [Online] 6 January 2025. [Cited: 3 March 2025.] https://www.gov.uk/government/news/joint-expeditionary-force-activates-uk-led-reaction-system-to-track-threats-to-undersea-infrastructure-and-monitor-russian-shadow-fleet.

Government Offices of Sweden. 2024. Statements. *Joint statement, Nordic-Baltic Summit at Harpsund.* [Online] 27 November 2024. [Cited: 2 January 2025.] https://www.government.se/statements/2024/11/joint-statement-by-the-heads-of-government-of-denmark-estonia-finland-latvia-norway-poland-and-sweden/.

Hoffman, Frank G. 2007. *Conflict of the 21st Century - The Rise of Hybrid Wars.* Arlington : Potomac Institute for Policy Studies, 2007.

JEF. 2025. About the JEF. *Joint Expeditionary Force.* [Online] 2025. [Cited: 25 January 2025.] https://jefnations.org/about-the-jef/.

Johanson, Art. 2021. *General Nikolai Reek on Operations and Leadership - Including Operation Albion and Battle of Cesis.* Tartu : Baltic Defence College, 2021.

Joint Forces. 2024. Joint-Forces.com. *Special Forces.* [Online] 7 January 2024. [Cited: 30 December 2024.] https://www.joint-forces.com/special-forces/70174-estonian-special-operations-command-exercise.

Kaitseliidu peastaap. 2024. *Kaitseliidu Arengukava 2035.* Tallinn : s.n., 2024.

Kaitseliit. 2024. Saaremaa Malev. *Ajalugu.* [Online] 30 12 2024. [Cited: 31 12 2024.] https://saaremaa.kaitseliit.ee/et/ajalugu.

Laanemets, Ott. 2021. Sea Power in the Baltic Sea. *Sõjateadlane (Estonian Journal of Military Studies).* 2021, Vol. 16.

Leskinen, Jari. 1999. *Veljien valtiosalaisuus.* Helsinki : WSOY, 1999.

Lucas, Edward, Hodges, Ben and Schmiedl, Carsten. 2022. *Close to the Wind: Recommendations for Baltic Sea Regional Security.* s.l. : Center for European Policy Analysis (CEPA), 2022.

Maps on the web. 2022. Baltic Sea Shipping Density. *Maps on the web.* [Online] 2022. [Cited: 25 February 2025.] https://64.media.tumblr.com/33772874b9a8cd8717da1b10ed8e1fb4/4446afe3f2686d64-e1/s1280x1920/f8295b9597d447ffe7d7cb4cdcea0afec3f202e9.jpg.

Mazarr, J Michael. 2018. Understanding deterrence. *RAND.* 2018.

NATO. 2022. *NATO 2022 Strategic Concept.* 2022.

—. 2017. News. *BALTOPS - a NATO maritime exercise with 46 years of history.* [Online] 10 Augusti 2017. [Cited: 31 December 2024.] https://www.ncia.nato.int/about-us/newsroom/baltops-a-nato-maritime-exercise-with-46-years-of-history#:~:text=Baltic%20Operations%20%28BALTOPS%29%2C%20an%20Allied%20maritime%20exercise%20taking,Originally%2C%20BALTOPS%20was%20exclusive%20to%20NATO%20Membe.

—. 2025. What is NATO? *About Us.* [Online] 2025. [Cited: 25 January 2025.] https://www.nato.int/nato-welcome/index.html.

Överbefälhavaren. 2024. *Försvarsmaktens strategiskaplan.* Stockholm : Försvarsmakten, 2024. FM2024-21844:1.

Pawlak, Julian. 2024. *Charting Challenges in the Baltic Sea.* s.l. : War on the Rocks, 2024.

Regeringen. 2022. *Ett försämrat säkerhetspolitiskt - Konsekvenser för Sverige.* Stockholm : Regeringskansliet, 2022. Ds 2022:7.

Reinventing Mine Warfare in the Baltic Sea. **Laanemets, Ott. 2024.** s.l. : U.S. Naval Institute, May 2024, Vol. 150.

Republic of Estonia Defence Forces. 2024. News. *Spring Storm gains momentum on the Islands.* [Online] 15 May 2024. [Cited: 29 December 2024.] https://mil.ee/en/news/spring-storm-gains-momentum-on-the-islands/.

Sliwa, Zdzislaw, Helseth, Hans and Veebel, Viljar. 2022. The Baltic Sea islands and their impact on the regional security. *Centrum Balticum Foundation.* 2022, 10.

The Russian Threat to Security in the Baltic Sea Region. **Stoicescu, Kalev.** s.l. : International Centre for Defence and Security.

Veebel, Viljar and Ploom, Illmar. 2019. Are the Baltic States and NATO on the right path in deterring Russia in the Baltic? *Defense & Security Analysis.* 35, 2019, Vol. 4.

Westberg, Jacob. 2023. *Svenska Säkerhetstrategier - Från neutralitetspolitik till ansökan om Natomedlemskap.* Lund : Studentlitteratur, 2023.

Wills, Steven. 2024. BALTOPS 24 in a Contested NATO Lake. *centerformaritimestrategy.org.* [Online] 18 June 2024. [Cited: 23 November 2024.] https://centerformaritimestrategy.org/publications/baltops-24-in-a-contested-nato-lake/.

MAJ Šarūnas Valiokas. What is the future of the Special Warfare? Is the current Allied Joint Doctrine for Special Operations still valid, or does it have to be adapted to contemporary military conflicts?

Introduction

"History is written by the victors", this quote raises a lot of discussion about which historical personality said it first, but in modern warfare, the history of victory is often shaped by the unseen hands of Special Operations Forces (SOF). Through covert operations and proactive military assistance, SOF has changed the definition of armed conflicts and significantly influenced world affairs. The main concern, however, is whether the NATO Allied Joint Doctrine for Special Operations (AJP-3.5), which was created for a different era, can keep up with these changing problems as warfare changes due to the emergence of hybrid threats, cyber warfare, and peer-to-peer competition.

SOF has always been driven by the concept of bottom-up adjusting to the needs of the contemporary situation. These forces have shown remarkable adaptability and strategic accuracy in everything from undermining enemy objectives during World War II to counterinsurgency operations in Vietnam and Afghanistan and emerged tasks and demands for SOF by the revival of high-intensity conflicts, such as the present conflict between Russia and Ukraine. Operations increasingly involve more than just traditional warfare; they now involve gathering intelligence, developing cyber capabilities, and aiding resistance organisations. Therefore, the before mentioned capabilities and expanded tasks necessarily have to be touched in the doctrine (Dieanu, 2022) (Borsari, 2022).

Although the Allied Joint Doctrine for Special Operations has helped NATO SOF communicate and work together, others contend it is still static, primarily preoccupied with stability and counterterrorism, and unsuitable for hybrid and multi-domain conflict. According to opposing viewpoints, SOF's counterterrorism expertise could make them less successful in peer-to-peer confrontations where conventional forces predominate (Hooker, 2023). Furthermore, operational fatigue and potential reduction of effectiveness can be an outcome of forces being in continual high-intensity operations. Therefore, the purpose of this paper is to make the case that SOF is still a useful and efficient tool to accomplish operational goals and to verify that the primary tasks of SOF as outlined in NATO Allied Joint Publication - 3.5 (AJP-3.5) Allied Joint Doctrine for Special Operations is still relevant but need to be updated and modified to reflect the demands of the modern battlefield and emerging threats.

The study is organized as follows: first, historical information about SOF, followed by how doctrine evolved in response to changing threat situations. Second, how special operations are defined in the Allied Joint Doctrine for Special Operations through core tasks dedicated to NATO SOF. Third, what are the challenges in modern combat when deploying SOF as an adaptive tool? There will be opposing viewpoints on SOF employment in war and what is wrong with the doctrine. Finally, conclusions and recommendations from the presented information will be drawn.

Chapter 1. Historical Overview of Special Operations and Evolution of the Allied Joint Doctrine for Special Operations

1.1. World War II. The Genesis of Modern SOF

The unfavourable situation and initiative, inventive and non-traditional-minded individuals made an effort to birth of SOF during World War II. Unconventional warfare utilized organizations like the American Office of Strategic Services (OSS) and the British Special Air Service (SAS) to start the development of the tactics. While OSS agents penetrated occupied Europe, conducting sabotage operations and crucially supporting resistance forces, the SAS carried out audacious raids on Axis airfields in North Africa (Horn, Michael, Ben-Ari, 2018). These early missions showed how small, mobile forces could effectively disrupt adversary activities and influence strategic outcomes while being tactical level troops.

The successful 1940 attack on Fort Eben-Emael in Belgium was one of the Germans' most notable contributions to developing special operations concepts throughout the war. Within hours, the fortress's defence was destroyed when a small group of German paratroopers secretly landed on top of it using gliders. Skilled personnel capable of striking precisely where it was not expected demonstrated creative operation that served as a model for future SOF missions, emphasizing the value of speed, surprise, and tactical superiority.

The planning and execution of D-Day stands out as one of the most significant instances of Allied SOF's success during World War II. As an example of their capacity to function behind enemy lines in harsh circumstances, SOF cleared the path for Allied assaults through intelligence collection, sabotage, and direct action (Brands, Nichols, 2020). Similarly, SOF took part in Operation Market Garden, an ambitious but ultimately unsuccessful attempt to seize important bridges in the Netherlands. The mission demonstrated the strategic potential of SOF in complex, large-scale campaigns despite logistical and coordination issues. Also, Brandenburgers, the German Abwehr intelligence unit, used disguising tactics that could be compared with pseudo operations features. The goal was to infiltrate behind enemy lines disguised as local forces or civilians to gather intelligence, disrupt supply lines, and create confusion within enemy ranks.

These operations laid the foundation for modern SOF principles like adaptability, precision, speed, and strategic employment. The units used in a non-traditional way showed the evolving role of different tactics in achieving objectives that conventional forces without Special Forces roles could not accomplish.

1.2. The Cold War. Expansion into Counterinsurgency and Irregular Warfare

SOF capabilities significantly increased during the Cold War as superpowers attempted to influence proxy conflicts and suppress insurgencies. The U.S. Special Operations Forces played a crucial role in Vietnam, where their knowledge of unconventional warfare, intelligence gathering, and training local troops had a significant impact on the situation in the war (Eriksson, Pettersson, 2017). Similar to this, Soviet Spetsnaz forces showed the value of SOF in Afghanistan by carrying out clandestine operations to cut off Mujahedeen supplies and destroy important objectives (Hunter, 2021).

The discovery of SOF limitations in Cold War time, especially in prolonged, high-intensity conflicts, stressed the necessity for SOF to work in concert with conventional forces. Identified lessons on failure to accomplish strategic objectives in Vietnam still guide SOF deployment today (Hooker, 2023). Rhodesian Army special forces unit Selous Scouts from the Rhodesian Bush War (1964-1976) conducted pseudo-operations by disguising themselves as insurgents, showed the possibility for different warfighting with insurgency and was used as tactics in future conflicts (Causwell, 2018). These tactics created an opportunity to blend among insurgents and get access to human networks, gather information, and execute deliberate operations against guerrilla forces.

1.3. Development of the Allied Joint Doctrine for Special Operations

NATO created the Allied Joint Doctrine for Special Operations (AJP-3.5) to address the difficulties of multinational operations. By standardising SOF operations across member states, the doctrine ensured interoperability, strategic accuracy and flexibility. Aware of the ability of Soviet Spetsnaz forces to engage in sabotage and asymmetric activities, the plan was to use SOF to gather sensitive information and disrupt plans. During the Cold War, NATO SOF was a very valuable tool for conducting operations behind enemy lines. The significance of SOF in handling the high-stakes atmosphere of ideological and military rivalry was highlighted by these missions

A demand for adaptable, agile troops that could function in complex and politically sensitive circumstances arose after the Cold War as the nature of global threats changed. The situation led to the formalization of AJP-3.5 in 2006, which reflected NATO's emphasis on joint operations and interoperability in the fight against irregular warfare and terrorism. The doctrine placed a strong emphasis on flexibility in order to handle the difficulties presented by hybrid threats, including information warfare, cyber operations, and the blending of conventional and unconventional tactics. These improvements made it possible for NATO SOF to continue being a strategic asset that could handle established and new security risks (De Wijk Rob et al., 2021).

1.4. Adapting to 21st Century Threats

NATO SOF was significantly involved in counterterrorism and stability operations in the early 21st Century, especially in Afghanistan and Iraq. Although SOF actions demonstrated the doctrine's usefulness in countering insurgency threats, they also exposed its shortcomings in preparing SOF for hybrid and high-intensity wars. The need for a more adaptable doctrine could be identified by the revival of state-on-state combat, as seen by the Russia-Ukraine conflict. Operations of the Ukrainian SOF, such as sabotage and intelligence gathering against Russian troops, show how special operations in contemporary warfare are changing (Borsari, 2022) (Dieanu, 2022).

The SOF's history highlights its strategic value and adaptability. The Allied Joint Doctrine for Special Operations, however, probably needs an update to address emerging threats and real-world operational challenges in modern warfare. It will be necessary to re-evaluate thoroughly NATO SOF's doctrine, capabilities, and integration with conventional forces to guarantee its continued effectiveness in both established and emerging tasks.

Chapter 2. Core tasks of Special Operations Forces defined in The Allied Joint Publication 3.5 (AJP-3.5) Allied Joint Doctrine for Special Operations

The historical evolution of SOF, as explored in Chapter 1, demonstrates how special operations have continuously adapted to shifting strategic environments. From World War II to the Cold War and beyond, SOF has refined its tactics and capabilities to meet emerging threats. This evolution has culminated in the NATO Allied Joint Publication 3.5 Allied Joint Doctrine for Special Operations (AJP-3.5 Doctrine), which serves as the foundation for defining the core tasks of modern SOF. As conflicts become increasingly hybrid and multi-domain, it is essential to assess whether these core tasks remain relevant and sufficient for contemporary warfare.

The AJP-3.5 Doctrine outlines core tasks for Special Operations Forces (SOF) that are essential for addressing contemporary security challenges and enhancing operational effectiveness. Conducting special operations, which are defined as military activity executed by small, specially selected, trained and equipped groups acting in unconventional ways and applying non-standard techniques, rely on doctrine that serves as a foundational document for NATO SOF, delineating core tasks, which include direct action (DA), special reconnaissance (SR), and military assistance (MA). Each of these tasks is designed to leverage the unique capabilities of SOF in various operational environments (AJP-3.5, 2019). For instance, direct action involves precise strikes against high-value targets, while special reconnaissance focuses on gathering critical intelligence in hostile areas. The doctrine emphasizes the importance of these tasks in enabling NATO SOF to operate effectively across a spectrum of conflicts. To achieve strategic impact while being precise and versatile, SOF has to use the essence of tasks as a foundation for Special operations.

2.1. Direct Actions (DA)

DA is a fundamental SOF task designed for rapid, high-precision operations that aim to achieve immediate tactical and strategic effects. DA missions include targeted strikes, hostage rescue, and sabotage operations. These operations require thorough planning, intelligence gathering, and coordination with other military branches to ensure success. Doctrine highlights DA as crucial in high-intensity conflict scenarios where speed, agility, and surprise provide a strategic advantage (AJP-3.5, 2019), whereas, at that time, conventional forces may face limitations. By employing small, agile units capable of executing precision strikes, SOF can disrupt enemy operations and create opportunities for larger conventional forces to exploit (AJP-3.5, 2019). However, the growing complexity of hybrid warfare necessitates an expansion of DA capabilities beyond traditional kinetic engagements.

For example, the Ukrainian SOF has adapted DA techniques to conduct sabotage operations behind enemy lines, disrupting Russian logistics and command structures. This demonstrates that DA is no longer confined to conventional military objectives but is increasingly integrated with cyber warfare and intelligence operations. As adversaries develop resilient countermeasures, SOF must refine DA approaches, incorporating emerging technologies such as AI-driven targeting and autonomous drone strikes. This synthesis suggests that DA may need to be rethought in the broader context of multidisciplinary activities. This synthesis underscores the need to rethink DA within a broader, multi-domain operational context. Direct Action remains a cornerstone of SOF capabilities, particularly in operations dedicated to high-value target neutralization.

2.2. Special reconnaissance (SR)

Special reconnaissance (SR) is crucial for providing timely and accurate intelligence that informs decision-making at all levels of command. The role of SR within NATO SOF is essential for understanding the operational picture and predicting the enemy's actions. Doctrine stresses the importance of SR missions in gathering intelligence on enemy movements, capabilities, and intentions (AJP-3.5, 2019). This task often involves deploying SOF teams into contested or denied areas to collect information that can significantly influence the outcome of larger military operations. By integrating advanced surveillance technologies and traditional reconnaissance techniques, SOF enhances situational awareness and supports strategic planning.

SR has traditionally provided battlefield intelligence for operational planning, but in an era of digital warfare, its role has expanded beyond physical reconnaissance. The ability to disrupt enemy communications and conduct cyber-enabled intelligence-gathering has become as critical as traditional SR missions. As demonstrated in Ukraine, where SOF leveraged electronic warfare and satellite reconnaissance to guide precision strikes, the doctrine must acknowledge these evolving dimensions of SR.

2.3. Military Assistance (MA)

Military assistance is a core task defined in the doctrine that emphasizes the role of SOF in supporting partner nations to enhance their military capabilities and resilience against threats. MA encompasses a range of activities designed to strengthen the defence capabilities of allied and partner nations. Doctrine outlines this task as vital for fostering stability and security in regions where conventional forces may not be present or effective (AJP-3.5, 2019). SOFs are unique to assist due to their specialized training, cultural awareness, and ability to operate in complex environments. This task can include training local forces, providing logistical support, and facilitating intelligence sharing to enable partner nations to address their security challenges independently.

An analysis of MA reveals a gap in its effectiveness in hybrid conflicts, necessitating a refined approach to counter evolving adversarial tactics. In Ukraine, SOF has played a crucial role in training local forces and enabling resistance operations in occupied territories. However, adversaries have adapted through countermeasures such as disinformation campaigns and infiltration tactics, underscoring the need for MA to integrate psychological operations and counter-information warfare strategies. Unlike previous SOF-led training missions focused on stability operations, MA now involves preparing partner forces to counter hybrid threats, including cyber-attacks and state-sponsored insurgencies. This shift is evident in NATO's support for the Ukrainian SOF, where training programs emphasize resilience against state-sponsored aggression. To ensure effectiveness, MA might incorporate the development of resistance networks and leverage decentralized command structures to counter adversarial suppression efforts. The doctrine might reflect a shift, aligning MA with broader strategic competition objectives to enhance partner forces' ability to resist kinetic and non-kinetic threats.

2.4. Interdependence of core tasks

The seamless integration of DA, SR, and MA ensures that SOF can address complex difficulties on the current battlefield. For example, during the Afghan conflict, SOF used SR and DA to locate and destroy high-value targets while also performing MA to prepare Afghan security forces for autonomous operations (Briscoe et al., 2003). In the continuing conflict in Ukraine, SR missions frequently precede DA operations like drone strikes or sabotage missions, resulting in a synergistic impact.

2.5. Adopting core tasks to Modern Warfare.

Changing the security environment concerning hybrid tactics and cyber threats influences operations planning and execution in all security forces, as well as SOF task accomplishing. Utilising cyber capabilities in SR operation demonstrated a very important asset in reducing the opponent's proper communication work, which disrupted coordination and, as a secondary effect, logistics that was possible to see in Ukraine. With ongoing development in the technological sphere, using space forces capabilities provides more measures to accomplish precise strikes on target and avoid collateral damage.

Chapter 3. Challenges in High-Intensity Conflict and Modern Warfare

While Chapter 2 outlined the key responsibilities of SOF under the AJP-3.5 doctrine, the effectiveness of these tasks is heavily influenced by the realities of modern warfare.

The ability of SOF to execute Direct Action, Special Reconnaissance, and Military Assistance is challenged by emerging threats, operational fatigue, and the increasing complexity of multi-domain operations. For the successful continuation of activities, it is crucial to examine the operational challenges that SOFs face in high-intensity and hybrid warfare scenarios.

One of the most pressing issues is the over-extension of SOFs in high-intensity conflicts. While SOFs excel in executing precision strikes and intelligence-driven operations, their effectiveness diminishes in protracted, large-scale combat. The operational fatigue resulting from continuous deployment poses a risk to long-term mission success (Hooker, 2023). To mitigate this, NATO should adopt a rotational deployment model, ensuring that SOF units maintain peak performance while leveraging conventional forces for sustained operations. Moreover, hybrid warfare demands a redefinition of SOF’s operational framework. The fusion of cyber operations, electronic warfare, and conventional tactics creates an environment where SOF must navigate multiple domains simultaneously. Integrating SOF within joint multi-domain operations is imperative, ensuring that these forces remain a decisive asset in contested battlespaces.

3.1. Limitations of SOF in prolonged military actions

Considerable challenges for SOF present high-intensity warfare when conventional forces dominate in prolonged large-scale battles. The operational pace can create limitations; SOFs are suited for small-unit tactics and precise strikes, but they suffer in long-lasting engagements with high death rates (Altman, 2024). Conventional forces' combined firepower can overwhelm SOF capabilities, which are frequently designed for quick, focused operations rather than long-term, high-casualty situations. Over time, this imbalance might influence SOF personnel efficiency due to operational fatigue, especially if they are working on tasks that are typically dedicated to bigger conventional groups (Hooker, 2023).

While SOF may face challenges in prolonged high-intensity engagements, these limitations become even more apparent in the evolving landscape of hybrid warfare. As adversaries increasingly blend conventional and unconventional tactics across multiple domains, SOF must continuously adapt to maintain operational effectiveness.

Variously used enemy tactics raise the question of how NATO SOF can remain agile in the face of hybrid warfare threats.

3.2. Hybrid warfare and Multi-domain operations

The modus operandi of NATO SOF must adapt to deal with complex threats in hybrid warfare, which are not foreseen in regulations and doctrines. In order to adapt to new kinds of conflict that involve several domains: land, sea, air, space, and cyber, SOF has to understand hybrid warfare, which blends traditional military strength with irregular tactics, cyber operations, and information warfare (Pomerleau, 2024). The strategic employment of SOF is made more difficult by this comprehensive approach, which requires them to resist state and non-state actors who take advantage of weaknesses in each area while integrating skills across different domains (Hoffman, 2007). The consequences for NATO SOF not only focus on kinetic operations but also include the requirement for improved cyber operations training and a stronger focus on obtaining intelligence to support multi-domain plans (Kinkead et al. 2024).

Furthermore, joint operations require improved interoperability among participating states' SOFs. Sharing practical insights and real-time intelligence on successful actions across different domains can enhance the ability to counter hybrid threats effectively. Synchronization of operations can significantly improve the impact of NATO SOF.

In addition to hybrid threats posed by state actors, NATO SOF must also contend with the increasing role of non-state actors in modern conflicts. These groups, often operating beyond traditional military structures, utilize guerrilla tactics, cyber-attacks, and propaganda to challenge conventional forces. As a result, SOF must refine their approach to countering asymmetric threats while ensuring their core tasks remain adaptable to state and non-state adversaries.

3.3. Asymmetric threats and non-state actors

Nowadays, challenges given by non-state actors and asymmetric threats emphasise the need for the AJP-3.5 doctrine to show flexibility and adaptability in counterterrorism operations. Non-state actors mainly operate outside of standard military frameworks, using guerrilla tactics, terrorism, and other unconventional approaches that can undermine conventional military responses.

Ongoing counterterrorism operations in Africa and the Middle East demonstrate how SOF can effectively confront these threats where conventional forces may fail (Tenenbaum, 2023). In many cases, these places are marked by complicated social and political processes that make military interventions difficult. SOF uses their agility and specialized training to carry out targeted operations against decentralised adversary networks. For example, they could gather intelligence to identify key leaders within terrorist organizations or direct action missions to destroy high-value targets. Also, Human Network Targeting presents significant challenges for SOF operators. Identifying key individuals within decentralized and clandestine networks requires extensive intelligence fusion from multiple sources, including human intelligence (HUMINT), signals intelligence (SIGINT), and cyber surveillance. Moreover, adversaries are increasingly aware of SOF tactics, employing deception, misinformation, and secure communication channels to evade detection. Furthermore, SOF's capacity to collaborate with local troops makes them more effective in these circumstances. NATO SOF can assist in the long-term development of indigenous capabilities by training and advising local security forces. This method not only addresses immediate risks but also adds to stability initiatives in these regions.

A recent and highly relevant example of SOF adapting to asymmetric threats and hybrid warfare can be seen in the ongoing Russia-Ukraine conflict. Ukrainian SOF has demonstrated how special operations can effectively challenge a conventional military force through sabotage, intelligence collection, and disruption of enemy logistics. Analysing these operations provides valuable insights into how NATO SOF may need to adapt their doctrine for future conflicts.

3.4. Role of SOF in high-intensity conflict: Case study of Ukraine

The ongoing conflict in Ukraine provides a compelling case study for analysing the adaptability and effectiveness of NATO's AJP-3.5 Doctrine in contemporary warfare. Ukrainian SOF has demonstrated remarkable versatility across a range of operations, aligning with and expanding upon the core tasks outlined in the doctrine.

In the early stages of the conflict, the Ukrainian SOF played a pivotal role in disrupting Russian forces near Kyiv, including operations in Hostomel (Mixailova, 2024), which delayed and disorganized Russian troop movements. These missions exemplify DA by targeting high-value objectives with precision, directly impacting the strategic calculus of the adversary. Similarly, sabotage missions against Russian supply convoys and command centres further highlight the critical role of DA in undermining enemy logistics and operational cohesion.

Special Reconnaissance has also been a cornerstone of Ukrainian SOF operations. Units from the Artan and Stugna groups conducted raids and intelligence-gathering missions on the occupied Crimean peninsula (Roshchina, Romanenko, 2023), providing actionable intelligence for subsequent strikes. These efforts were complemented by psychological operations behind enemy lines, which sowed confusion among Russian forces and bolstered Ukrainian resistance efforts. The integration of traditional SR methods with advanced technologies, such as electronic warfare and satellite reconnaissance, underscores the evolving nature of this task in hybrid warfare.

Military Assistance has been equally significant in Ukraine's defence strategy. Ukrainian SOF has closely collaborated with Territorial Defence Forces to enhance their capabilities, providing training, operational support, and coordination in contested areas. This partnership has been instrumental in leveraging local knowledge and manpower to counter Russian advances effectively. Moreover, the Ukrainian SOF extended their reach beyond national borders by conducting operations in Sudan to undermine Russian influence and disrupt Wagner Group activities, showcasing the global implications of modern MA efforts.

The Ukrainian SOF played a crucial role in executing unconventional tactics in Kherson district. They were instrumental in planning and carrying out sabotage missions, training local populations for partisan warfare, and implementing innovative combat strategies. Their expertise allowed for the effective disruption of Russian operations and contributed significantly to the successes in battles like Chornobaivka (Yaffa, 2025).

Finally, the Ukrainian SOF has demonstrated operational flexibility through amphibious raids on islands in the Black Sea (Romanenko, 2022) and Dnipro River (Balachuk, 2023) regions. These actions disrupted Russian naval operations and showcased the ability of SOF to operate effectively across multiple domains. These examples collectively highlight the relevance of NATO's AJP-3.5 doctrine while also pointing to areas where it may require updates, particularly in addressing multi-domain operations, cyber-enabled capabilities, and partnerships with non-traditional forces.
This case study illustrates that while NATO's core doctrinal tasks remain relevant, their application must evolve to meet the demands of hybrid conflicts like those seen in Ukraine. The adaptability displayed by the Ukrainian SOF offers valuable lessons for refining NATO doctrine to ensure its continued effectiveness in modern warfare scenarios.

This paragraph synthesizes doctrinal analysis with real-world examples from Ukraine to provide a focused discussion on how NATO's AJP-3.5 doctrine applies to contemporary conflicts. It highlights successes and areas for potential doctrinal adaptation while maintaining coherence with the broader themes of the research paper.

Chapter 4. Debating the Future of NATO SOF

As Chapter 3 highlighted the operational challenges faced by SOF in modern conflicts, it is necessary to consider alternative perspectives on the effectiveness of NATO’s current doctrine. While the AJP-3.5 doctrine provides a structured approach to SOF employment, critics argue it remains overly rigid in addressing emerging threats. Alternative viewpoints suggest that the doctrine must evolve to reflect the realities of hybrid warfare, emphasizing adaptability over standardized methodologies (Votel et al., 2016).

Some analysts contend that SOFs are best suited for counterterrorism and irregular warfare rather than state-on-state conflicts (Fabian, 2018). This perspective highlights the potential risks of over-relying on SOF in conventional battles, where mass forces and sustained logistics play a more decisive role. However, as evidenced by the Ukraine conflict, SOF’s ability to conduct unconventional operations against conventional forces suggests that their role in modern warfare extends beyond traditional counterterrorism missions.

Additionally, concerns about operational fatigue underscore the necessity for more sustainable deployment strategies. SOF should not be the default solution for every crisis; their employment must be balanced with broader military assets (Leebaert, 2007). By refining doctrine to incorporate these critiques, NATO can ensure that SOF remains an agile and effective force capable of addressing 21st-century security challenges.

4.1. Speculations about the Allied Joint Doctrine for Special Operations is being too static and does not fully address the evolving nature of modern, hybrid warfare

The existing Allied Joint Doctrine for Special Operations, while foundational, is often criticized for its rigidity. Alternative opinion owners argue that the doctrine lacks the flexibility to respond to the rapidly evolving character of modern hybrid warfare, influenced heavily by technological advancements and geopolitical shifts. Scholars like Michael G. Vickers emphasize that hybrid warfare demands adaptive frameworks integrating emerging domains such as cyber and space operations (Votel et al., 2016). Without updates, the doctrine risks fostering a static approach that could hinder adequate preparation for diverse and fluid threats.

While critics argue that the AJP-3.5 doctrine is rigid, NATO SOF has continuously adapted operational methods in response to emerging threats. As seen in Ukraine, SOF has successfully integrated cyber operations, space-based intelligence, and electronic warfare into their missions (Neag, Solescu, 2024). The doctrine provides a necessary framework, but flexibility is built into SOF training and execution, allowing them to operate beyond conventional doctrinal constraints (Buckingham et al., 2023).

4.2. SOF is best suited for counterterrorism and irregular warfare

A segment of military analysts contends that SOF's specialized capabilities are most effective in counterterrorism and irregular warfare scenarios (Fabian, 2018). In these contexts, SOF agility, precision, and adaptability are maximised. However, there are some analysts, including Linda Robinson, argue that SOF may not be ideally suited for large-scale state-on-state conflicts (Robinson, 2015). For example, the strategic demands of direct peer-to-peer warfare often require mass forces and sustained logistics that fall outside the typical SOF operational profile. This critique warns against overextending SOF capabilities into roles that may dilute their effectiveness.

Modern SOFs are not limited to counterterrorism; they have played critical roles in peer-to-peer conflicts, such as intelligence gathering, deep strikes, and supporting resistance movements. The Ukrainian SOF have demonstrated effectiveness in disrupting conventional Russian military operations, showing that SOF can function in large-scale conflicts. Integrating SOF into multi-domain operations ensures their relevance beyond counterterrorism, including strategic reconnaissance, sabotage, and resistance warfare. NATO SOF’s ability to conduct special operations in denied areas makes them indispensable in high-intensity conflicts.

4.3. The over-reliance on SOF has led to operational fatigue

The continuous global demand for SOF's specialized skills has resulted in operational fatigue across many units. This fatigue, compounded by extensive worldwide deployments, risks diminishing their long-term effectiveness. As Derek Leebaert highlight the dangers of over-reliance on SOF, cautioning that without adequate operational cycles and integration with conventional forces, SOF may struggle to sustain their elite performance (Leebaert, 2007). This perspective underscores the importance of balancing SOF missions with broader force integration and sustainable support structures.

While operational fatigue is a valid concern, NATO has taken steps to ensure sustainable force employment through rotational deployments and force modernization. Increased cooperation with conventional forces allows SOF to focus on specialized missions rather than being overburdened with conventional combat roles. Expanding hybrid warfare training and leveraging technology (e.g., AI-driven intelligence, drone warfare) reduces physical strain on SOF operators. The strategic value of SOF justifies their frequent use, but efforts are continuously made to balance deployments and preserve force effectiveness.

The rapidly changing situation in the nature of warfare necessitates the re-examining of NATO’s SOF doctrine to enhance its adaptability and effectiveness. While AJP-3.5

provides a foundational framework, it must integrate lessons from recent conflicts, including the Ukraine war, to refine SOF tasks. Incorporating doctrinal refinements will ensure that NATO SOF remain a decisive instrument in modern warfare, capable of responding to unconventional and conventional threats with agility and precision.

Conclusions

The historical trajectory of SOF illustrates their irreplaceable role in shaping military outcomes through unconventional tactics and strategic flexibility. However, as contemporary conflicts increasingly blend traditional and non-traditional warfare elements, the current AJP-3.5 doctrine may require further adaptation to address these complexities fully. The rise of hybrid warfare necessitates a revaluation of SOF capabilities and operational frameworks, particularly concerning the possible integration of pseudo-operations for covert missions where SOF personnel disguise themselves as enemy forces to gather intelligence or disrupt enemy actions. Such tactics have proven effective in past conflicts and might be formally incorporated into the doctrine to enhance SOF adaptability in contested environments.

Moreover, intelligence sharing remains a pressing issue within NATO operations. Effective collaboration among member states is paramount for timely and accurate intelligence dissemination, directly influencing operational success. Fluent state cooperation is directly dependent on intelligence sharing mechanisms that influence timely dissemination among allied state SOF execution of strategic tasks is limited by doctrine. This is particularly relevant in high-stakes scenarios where rapid decision-making is crucial, such as the ongoing conflict in Ukraine, where SOF have demonstrated intelligence gathering capacity to inform broader strategic objectives.

In addition to these operational considerations, aligning SOF practices with technological advancements is essential for maintaining relevance in modern warfare. Integrating high-end technologies, such as sophisticated surveillance systems, cyber capabilities, and artificial intelligence, into SOF operations can significantly enhance their effectiveness. The doctrine must evolve to incorporate these innovations while ensuring that personnel are adequately trained to utilize them effectively. This alignment will not only improve situational awareness but also facilitate more precise execution of missions in complex operational environments.

While NATO's AJP-3.5 doctrine has provided a foundational framework for SOF operations, it must undergo significant revisions to remain relevant amidst the rapidly changing nature of warfare. Including SOF in multi-domain operations guarantees its applicability outside counterterrorism in strategic reconnaissance, sabotage, and resistance warfare. By incorporating pseudo-operations into its core tasks, enhancing intelligence-sharing protocols among member states, and leveraging technological advancements, NATO can ensure that its Special Operations Forces continue to serve as a vital asset in achieving strategic objectives across diverse conflict scenarios.

Recommendations

To enhance the effectiveness of NATO SOF in contemporary military operations, several recommendations are proposed:

1. Revise the AJP-3.5 Doctrine: A comprehensive review and update of the AJP-3.5 doctrine is essential to incorporate lessons learned from recent conflicts and emerging threats. This revision should focus on integrating hybrid warfare strategies encompassing cyber capabilities, information warfare, and multi-domain operations.
2. Enhance Training for Unconventional Warfare: Training programs for SOF should be expanded to include advanced cyber operations and intelligence gathering techniques tailored for hybrid threats. This will enable SOF to operate effectively across various domains and counter state and non-state actors.
3. Increase Interoperability among Forces: Efforts should be made to improve interoperability within NATO and with partner nations' forces. Joint exercises that simulate hybrid conflict scenarios can foster collaboration and enhance operational readiness.
4. Address Operational Fatigue: Strategies must be implemented to mitigate operational fatigue among SOF personnel. This includes rotating forces more frequently in high-intensity environments and ensuring adequate rest periods to maintain effectiveness.
5. Leverage Technological Advancements: Investing in new technologies that enhance surveillance, reconnaissance, and communication capabilities will provide

SOF with a tactical edge in modern combat scenarios. Emphasizing innovation can help adapt traditional practices to contemporary needs.

Summarising, while NATO's SOF have proven their strategic value over decades of conflict, adapting their doctrine and operational practices is crucial for maintaining relevance in an increasingly complex security environment. By addressing these recommendations, NATO can ensure that its Special Operations Forces remain practical tools for achieving operational goals in future military engagements.

Bibliography

AJP-3.5, NATO Standardization Office (NSO). 2019. NATO Allied Joint Publication. AJP-3.5. Allied Joint Doctrine for Special Operations. [Online]. 2019. Vol. Edition B Version 1. [Cited : 25 October 2024]. https://www.coemed.org/files/stanags/01_AJP/AJP-3_EDC_V1_E_2490.pdf

ALTMAN, Howard. 2024. American Special Operations Forces Are At A Crossroads. *The Warzone*. [Online]. 2024. [Cited : 14 January 2025]. https://www.twz.com/news-features/american-special-operations-forces-are-at-a-crossroads

BALACHUK, Iryna. 2023. Manoeuvring on two boats: Special Operations Forces show how they defeated invaders on one of Dnipro River islands. *Ukrainska Pravda*. [Online]. 13 July 2023. [Cited : 14 March 2025]. https://www.pravda.com.ua/eng/news/2023/07/13/7411227/

BORSARI, Federico. 2022. Hunting the Invader: Ukraine’s Special Operations Troops. [Online]. 2022. [Cited : 15 November 2024]. https://cepa.org/article/hunting-the-invader-ukraines-special-operations-troops/

BRANDS, Hal and NICHOLS, Tim. 2020. Special Operations Forces and Great-Power Competition in the 21st Century. American Enterprise Institute. *AMERICAN ENTERPRISE INSTITUTE*. [Online]. 2020. [Cited : 20 January 2025]. https://www.aei.org/research-products/report/special-operations-forces-and-great-power-competition-in-the-21st-century/

BRISCOE, CHARLES H., KIPER, RICHARD L., SCHRODER, JAMES A., SEPP, KALEV I. 2003. Weapon of choice : U.S. Army Special Operations Forces in

Afghanistan. *Fort Leavenworth, KS : Combat Studies Institute Press, US Army Combined Arms Center,*. [Online]. 2003. [Cited : 2 February 2025]. https://cgsc.contentdm.oclc.org/digital/collection/p16040coll3/id/273/

BUCKINGHAM, Maike, DEMPSEY, William, DYAL, Justin, JAMES, Bobby, MARSH, Dr. Christopher, et al. 2023. *Special operations forces reference manual*. Fifth edition. MacDill Air Force Base, Florida: JSOU Press. ISBN 978-1-941715-58-1.

CAUSWELL, Xander. 2018. The Logic of Pseudo-Operations: Lessons from the Rhodesian Bush War. *Georgetown Security Studies Review*. [Online]. 2018. [Cited : 20 January 2025]. https://georgetownsecuritystudiesreview.org/2018/05/31/the-logic-of-pseudo-operations-lessons-from-the-rhodesian-bush-war/?utm_source=chatgpt.com

COL. BERT E. KINKEAD, RETIRED, Col. Jamie C. Riesberg, Lt. Col. Cynthia A. Facciolla, Lt. Col. Bobbi S. Snowden, DrPH, Master Sgt. Jan M. Krieg, 2024. Pursuing Global Impact Special Operations Forces' Vital Role in Achieving Objectives Through Global Health Engagement Initiatives. *Army University Press*. [Online]. 2024. [Cited : 20 January 2025]. https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/Nov-Dec-2024/Pursuing-Global-Impact/

DE WIJK ROB, FRANK, Bekkers, STEPHAN, De Spiegeleire, TIM, Sweijs and DORITH, Kool. 2021. The Future of NLD SOF: Towards an All-Domain Force. *The Hague Centre of Strategic Studies*. [Online]. 2021. [Cited : 20 January 2025]. https://hcss.nl/wp-content/uploads/2021/07/Future-of-SOF-20210629-final-revisions-FB.pdf

DIEANU, Adrian-Corneliu. 2022. The Role of Ukrainian Special Operations Forces Within the War in Ukraine. *International Scientific Conferince "StrategiesXXI."* 6 December 2022. Vol. 18, no. 1, pp. 220–228. DOI 10.53477/2971-8813-22-26.

ERIKSSON, Gunilla and PETTERSSON, Ulrica. 2017. *Special Operations from a Small State Perspective*. [Online]. [Cited : 20 January 2025]. New Security Challenges. https://link.springer.com/book/10.1007/978-3-319-43961-7

FABIAN, Sandor. 2018. NATO Special Operations Forces: Even if It Is Not Broken Yet, It Needs to Be Fixed. *Special Operations Journal*. 3 July 2018. Vol. 4, no. 2, pp. 188–201. DOI 10.1080/23296151.2018.1511084.

HOFFMAN, Frank G. 2007. Conflict in the 21st Century: The Rise of Hybrid Wars. *Potomac Institute for Policy Studies*. [Online]. 2007. [Cited : 20 November 2024]. https://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf

HOOKER, R.D. 2023. America's Special Operation problem. *Joint Force Quarterly*. [Online]. 2023. [Cited : 5 December 2024]. https://ndupress.ndu.edu/Media/News/News-Article-View/Article/3264605/americas-special-operations-problem/

HORN, Bernd, MICHAEL, Kobi and BEN-ARI, Eyal (eds.). 2018. *The evolution of SOF and the rise of SOF Power*. London New York, NY: Routledge, Taylor & Francis Group. Cass military studies. ISBN 978-1-315-20811-4.

HUNTER, Steve. 2021. A Leader's Perspective on Great Power Competition and SOF. *Kingston Consortium on International Security*. [Online]. 2021. Vol. I, no. 7. [Cited : 11 November 2024]. https://static1.squarespace.com/static/6034150d85deb0136ad574f2/t/618d229dbae9ea0b5292d1b4/1636639390122/KCIS+INSIGHTS+-+Hunter+1-7.pdf

JOSEPH L. VOTEL, CHARLES T. CONNETT, CHARLES T. CLEVELAND, and WILL IRWIN. 2016. Unconventional Warfare in the Gray Zone. *Joint Force Quarterly*. [Online]. 2016. [Cited : 25 January 2025]. https://ndupress.ndu.edu/Media/News/News-Article-View/article/643108/unconventional-warfare-in-the-gray-zone/

LEEBAERT, Derek. 2007. *To dare and to conquer: special operations and the destiny of nations, from Achilles to Al Qaeda*. 1st Back Bay pbk. ed. New York: Back Bay Books. ISBN 978-0-316-01423-6.

MIXAILOVA, Oksana. 2024. Пылали автобусы и самолеты: как защищали аэродром Гостомель и почему не удалось спасти Мрию. *Факты*. [Online]. 1 April 2024. [Cited : 14 March 2025]. https://fakty.com.ua/ru/ukraine/20240401-palaly-avtobusy-ta-litaky-yak-boronyly-aerodrom-gostomel-ta-chomu-ne-vdalosya-vryatuvaty-mriyu/

NEAG, Mihai Marcel and SOLESCU, Daniel. 2024. Analysis on the Actions of Ukrainian Special Operations Forces in the Russian-Ukrainian Conflict (February 2022

– February 2024). *International conference KNOWLEDGE-BASED ORGANIZATION*. 1 June 2024. Vol. 30, no. 1, pp. 129–135. DOI 10.2478/kbo-2024-0018.

POMERLEAU, Mark. 2024. Special ops expected to play key role in shaping future battlespaces in 'non-physical domains.' *DefenseScoop*. [Online]. 2024. [Cited : 20 January 2025]. https://defensescoop.com/2024/03/08/special-ops-role-shaping-future-battlespaces-non-physical-domains/

ROBINSON, Linda. 2015. One Hundred Victories: Special Ops and the Future of American Warfare. *Special Operations Journal*. 2 January 2015. Vol. 1, no. 1, pp. 69–71. DOI 10.1080/23296151.2015.1017988.

ROMANENKO, Valentyna. 2022. Operation Zmiinyi (Snake): Ukrainian Special Operations Forces reveal exclusive details of their landing on the island. *Ukrainska Pravda*. [Online]. 7 July 2022. [Cited : 14 March 2025]. https://www.pravda.com.ua/eng/news/2022/07/7/7356899/

ROSHCHINA, Olena and ROMANENKO, Valentyna. 2023. Ukrainian special operation forces land in Crimea, battle with losses occurs – Defence Intelligence. *Ukrainska Pravda*. [Online]. 4 October 2023. [Cited : 14 March 2025]. https://www.pravda.com.ua/eng/news/2023/10/4/7422614/

TENENBAUM, Élie. 2023. High-Intensity Warfare What Challenges for the French Armed Forces? *Security Studies Centre*. 2023.

YAFFA, Joshua. 2025. The Adventures of a Ukrainian Intelligence Officer. *The New Yorker*. [Online]. 24 February 2025. [Cited : 25 March 2025]. https://www.newyorker.com/magazine/2025/03/03/the-adventures-of-a-ukrainian-intelligence-officer

MAJ Martin Veermets. AI Use in Ukraine and Its Near Future Potential in Warfare

Introduction

Artificial Intelligence (AI) is rapidly reshaping the logistics of modern warfare, transforming how militaries manage sustainment, predictive maintenance, and frontline resupply. Among the most striking developments are AI-enabled predictive maintenance systems - like NATO’s CBM+ and ODIN - that minimise downtime and maximise equipment availability. Simultaneously, uncrewed systems such as autonomous drones and vehicles revolutionise last-mile delivery, ensuring agility and survivability in contested environments. (Gray, et al., 2021; Mitchell, 2023)

The ongoing war in Ukraine has emerged as a crucial real-time testbed for these AI applications. With supply chain fragmentation and dynamic battlefronts, Ukraine has accelerated the integration of AI tools such as the Brave1 platform and the Delta system. These technologies have enabled near real-time decision-making, resource allocation, and threat response - demonstrating how AI can enhance tactical resilience and strategic foresight. (Bondar, 2024; Goncharuk, 2024) This environment has influenced AI systems' development, evaluation, and enhancement, offering relevant answers to real-world issues. Can logistics be considered part of the mission outlined by Ukrainian general Valerii Zaluzhnyi, namely “searching for new and non-trivial approaches to break military parity with the enemy” (Zaluzhnyi, 2023)?

NATO, in parallel, is investing in AI through initiatives like DIANA and its Artificial Intelligence Strategy, viewing AI as a critical enabler for force mobility, predictive logistics, and autonomous sustainment. The convergence of military necessity and technological innovation - especially in Ukraine - signals that AI is not merely a support function but a potential multiplier that could redefine operational concepts and defence doctrines.

This research examines the growing role of AI in military logistics through two primary lenses: NATO's doctrinal trajectory and Ukraine's battlefield innovations. These two cases allow for a comparative analysis of emergent practices and future possibilities. This study is primarily descriptive and analytical. Rather than testing a hypothesis, it maps how AI transforms military logistics by examining emergent trends, their operational impacts, and the challenges of secure integration. The paper seeks to identify actionable insights and critical gaps in our current understanding through the comparative lens of NATO's doctrinal strategy and Ukraine's live conflict application.

While theories such as the Revolution in Military Affairs (RMA) suggest that AI represents a transformational shift in warfare, its long-term impact on sustainment strategies, force projection, and strategic autonomy remains underexplored (Raska, 2020). Despite the growing application of AI in defence, significant uncertainties persist about how scalable, dependable, and ethically tenable these systems are in real-world, long-term military operations. Much of the discourse so far has centred around technological potential. However, we still lack a clear understanding of how these tools behave in environments defined by persistent adversarial pressure, cyber threats, and resource volatility.

While Ukraine has demonstrated that AI can streamline logistics and support rapid battlefield responses, its long-term viability under continued stress remains unknown. Similarly, NATO's conceptual and doctrinal models are forward-looking but largely untested in active, high-intensity warfare. A grounded comparison is missing from the current discourse: how do strategic plans (NATO) and operational improvisations (Ukraine) reflect or contradict each other? Can they inform one another? More critically, do they adequately prepare us for the demands of future warfare?

This paper contributes to closing this gap by mapping observable trends, comparing distinct approaches, and identifying structural risks and integration challenges. It does so not by testing a single hypothesis but by presenting a layered descriptive analysis of developments still unfolding.

The growing complexity of military operations, especially in high threat, contested environments, compels a reassessment of how logistics are conceptualised and executed. AI technologies offer a toolkit to respond to these challenges, but their integration is not without friction.

This paper, to understand AI's transformative impact, proposes three interlinked research questions:

1. What are the trends of AI optimising military logistics operations?
2. How can these trends enhance military operations in rapidly evolving conflict environments?
3. How can AI-driven logistics be securely integrated into military operations?

These questions stem from the core problem outlined above: while AI is reshaping logistics, its reliability, resilience, and strategic implications must be unpacked more rigorously. By studying NATO's strategic developments and Ukraine's operational applications, the paper explores how theory meets practice - and where gaps persist.

This research examines AI's existing and prospective applications in military logistics, focusing on case studies from Ukraine and strategic models adopted by NATO. The study employs a qualitative methodology, integrating academic literature review (peer-reviewed journals, technical reports), defence publications, official NATO documents, and case studies.

Additionally, advanced search tools were utilised to source technical documents and detailed studies on specific AI systems in logistics, ensuring that the analysis is grounded in the most current and relevant research.

By comparing the innovations emerging from Ukraine's conflict with NATO's broader strategic initiatives, the study aims to identify transferable lessons and future trends that can inform military logistics and operational readiness in rapidly evolving conflict environments.

Section 1: Theory – the evolution of AI in warfare

Understanding the evolution of AI in warfare is essential to grasp the more profound implications of its use in military logistics. This section lays the study's theoretical foundation by showing how AI has developed from a support tool into a key driver of military transformation - mirroring earlier shifts such as mechanisation and airpower integration by framing AI within a broader historical and doctrinal arc to appreciate better its potential to reshape logistics processes and the strategic logic underpinning military operations. This theoretical lens sets the stage for analysing NATO's strategic ambitions and Ukraine's wartime innovations. More specifically, this study examines how the key characteristics of AI-driven military logistics identified in theoretical literature—such as predictive responsiveness, autonomous sustainment, and data-centric decision-making—are reflected conceptually in NATO's doctrinal framework and operationally in Ukraine's battlefield applications.

The development and application of AI in military operations can be viewed through the lens of technological revolutions in warfare - comparable to the mechanisation of armed forces during the Industrial Revolution or the introduction of airpower in World War II. The theoretical frameworks of Diffusion of Innovation and Principal-Agent Theory suggest that AI adoption in military sustainment will depend on institutional structures, technological readiness, and external strategic pressures. (Eisenhardt, 1989; Rogers, 2003) Therefore, this study seeks to analyse the role of AI in military logistics, assess its current and future potential in warfare, and explore the challenges associated with its widespread adoption. These frameworks help illuminate the contrasting dynamics between NATO's structured, multinational approach - where adoption is shaped by alliance-level bureaucracy and doctrine - and Ukraine's rapid, bottom-up implementation driven by immediate battlefield needs and innovation under pressure.

Early AI systems focused on automating routine tasks, but recent advances in machine learning, natural language processing, and autonomous systems have made AI a key enabler of dynamic battlefield functions. These include predictive maintenance, adaptive command decision-making, and autonomous logistics (Szabadföldi, 2021; Rashid, et al., 2023; Gilli, et al., 2025). Accordingly, this paper investigates how these capabilities are conceptualised within NATO's doctrinal developments and strategic frameworks.

This multi-tiered AI integration reflects a doctrinal evolution. Just as the advent of military aviation transformed airlift into a central sustainment capability, AI and robotics are transitioning from niche tools to central pillars of logistics (Stanley-Lockman, 2019). NATO's reviews confirm that AI can reduce equipment downtime, optimise inventories, and streamline logistics pipelines - benefits long proven in the commercial sector and now increasingly transferable to military use (Gray, et al., 2021).

In effect, AI is for logistics what mechanisation was for the Industrial Age – a catalyst for unprecedented efficiency gains (Trofymenko, et al., 2024; Lobariev, 2024).

Industrial Mechanisation (20th century)	**AI-Driven Logistics (21st century)**
Mass production and supply standardisation	Adaptive, autonomous supply optimisation
Mechanised transport and centralised hubs	Uncrewed logistics platforms and distributed systems
Reliance on human decision-makers	Increasing automation and AI decision support
Strategic shift: workforce to machinery	Strategic shift: human control to algorithmic coordination

Table 1. Historical analogy - mechanisation vs AI in military logistics. Based on Stanley-Lockman (2019), Gray et al. (2021), Trofymenko et al. (2024), and Lobariev (2024). The table was created by the author.

Drawing on the literature, the author has created Table 1. which provides a comparative framing to see how AI is not just automating logistics but is fundamentally reshaping the doctrine and tempo of sustainment, like how mechanisation changed warfare in the last century. However, this evolution also brings dilemmas: as human involvement is reduced, ethical and strategic oversight must increase (Johnson, 2020; Osinga, et al., 2021). This study uses this theoretical lens to explore whether, and to what extent, NATO and Ukraine are merely digitising logistics or fundamentally reimagining them.

Methodologically, the current study is primarily descriptive and exploratory - it aims to chart how AI-driven logistics are emerging, how they function in conflict settings, and what strategic, ethical, and operational implications they carry. The following sections were selected accordingly: NATO provides the doctrinal and strategic framework, Ukraine offers empirical evidence from ongoing conflict, and the integration and outlook section addresses the systemic challenges and potential risks. Together, these parts help us understand how AI is not just supplementing logistics - it increasingly defines how militaries think about sustainment, resilience, and operational tempo.

Section 2: NATO's AI in logistics

The following analysis identifies how these theoretical dimensions - predictive logistics, autonomous systems, and AI-enabled coordination - are embedded in NATO's strategic planning and logistical modernisation efforts. The section explores NATO's strategic vision for AI-enabled logistics and its relevance to future coalition warfare. It addresses the first research question by identifying prominent AI applications and how they are integrated across strategic, operational, and tactical levels. NATO's case is essential because it provides a doctrinally coordinated, multinational framework that anticipates future demands. The section sets a benchmark for comparison, allowing us to assess later whether Ukraine's battlefield solutions align with or challenge NATO's approach.

NATO views AI as a transformative force multiplier for military logistics, crucial to maintaining the Alliance's strategic edge in a fast-evolving security environment. In modern warfare, wars are decided not only by weapons and tactics but also by the agility and resilience of supply chains. By leveraging AI to enhance logistical efficiency, NATO aims to ensure its forces are supplied, sustained, and protected better than any adversary. (Gray, et al., 2021) This focus is vital: AI-optimised logistics bolsters operational readiness and credible deterrence, reinforcing NATO's ability to project power and sustain operations under the most demanding conditions. (NATO, 2024; Johnson, 2020; Osinga, et al., 2021)

Classical military theorists like Clausewitz and Jomini emphasised logistics as a critical enabler of war, arguing that supply chains determine the ability of an army to sustain operations (Erbel, et al., 2015). These theories are updated to incorporate supply chain management, resilience studies, and digitalisation. NATO's approach to integrating AI reflects this evolution: by enhancing logistics networks, predictive analytics, and autonomous resupply systems, AI is a critical enabler for maintaining force mobility and operational readiness in an increasingly complex global threat environment. (NATO, 2024; Trofymenko, et al., 2024)

NATO envisions AI applications supporting all three core tasks (collective defence, crisis management, and cooperative security) by enhancing mission support and operational logistics responsibly and interoperable. Its approach is very deliberate: it cannot innovate in AI and cybersecurity without private-sector input, and it fosters public-private collaboration through dedicated structures and initiatives (DIANA (NATO, 2021), NATO Innovation Fund (NATO, 2024), CCDCOE, the NATO Artificial Intelligence Strategy (NATO, 2024)), joint exercises, funding of startups, and direct integration of commercial AI tools into operational readiness pipelines. No longer are logistics just about moving fuel and ammunition; they now involve predictive algorithms, smart sensors, and autonomous delivery systems coordinating across strategic, operational, and tactical levels. At the strategic level, NATO is building AI-driven logistics networks for force mobility and prepositioning. At the operational level, machine learning forecasts demand and optimises resupply routes, improving battlefield sustainment. At the tactical level, autonomous platforms like uncrewed supply vehicles and drones provide last-mile delivery to frontline units in real time.

Several clear trends have emerged in how NATO is optimising logistics via AI:

1. Predictive Maintenance: NATO forces utilise AI for condition-based maintenance to optimise equipment availability. Machine learning algorithms use sensor data from aircraft and naval vessels to forecast breakdowns pre-emptively, facilitating timely repairs and parts replacement. An exemplary instance is the logistics system of the F-35 fighter. The Autonomic Logistics Information technology (ALIS) was replaced by the AI-enhanced Operational Data Integrated Network (ODIN), a cloud-based technology that markedly enhanced fleet preparedness by diminishing maintenance downtime. (Losey, 2022; F-35 Joint Program Office, 2022) NATO aims to reduce unforeseen equipment malfunctions, prolong platform longevity, and guarantee the availability of necessary material at the right time and location by utilising big data and predictive analytics. (Goncharuk, 2024). The system of record (CBM+) with an integrated AI and machine learning tool PANDA for predictive maintenance is also widely used (Mitchell, 2023). This transition exemplifies how AI-driven logistics systems can enhance sustainability and aircraft availability across Alliance militaries. (Kudzko, et al., 2023; Gray, et al., 2021)
2. Autonomous resupply and distribution: NATO is experimenting with autonomous transportation to move supplies more efficiently and safely. Semi-autonomous “leader-follower” convoys, where a convoy of uncrewed vehicles

follows a human-driven lead truck, have been tested by NATO armies to reduce risk to personnel and improve convoy throughput (Wakefield, 2021). Similarly, NATO allies are integrating uncrewed aerial systems for logistics. Cargo drones and uncrewed helicopters can deliver ammunition, food, or medical supplies to forward positions where traditional trucks might be too slow or vulnerable. Early exercise deployments have shown that autonomous resupply drones can cut delivery times and operate in contested airspace (Layton, 2021). NATO's vision of rapid force deployment heavily leverages such AI-enabled platforms – ensuring troops and materiel flow into theatre quickly, even under fire, reinforcing deterrence by denial (Olmstead, 2024). For instance, AI-optimised sustainment and drone logistics make it harder for adversaries to disrupt NATO's support lines, thus bolstering the Alliance's defensive posture (Wilner, et al., 2021).

3. Threat mitigation: AI is enhancing NATO logistics by providing end-to-end visibility of supply chains and guarding against disruptions. Advanced algorithms process logistics data to optimise routing, manage inventory levels across depots, and rapidly reallocate resources when demands spike. During extensive exercises, NATO logisticians have begun using AI decision-support tools to reroute shipments based on battlefield updates dynamically. Just as importantly, these AI systems help detect anomalies or threats to the supply chain. NATO's AI Strategy highlights the need for resilient autonomous networks (Gray, et al., 2021; NATO, 2024), and one focus area is using AI for the cyber defence of logistics - cyber resilience is now recognised as part of logistics readiness (exemplified by the annual Cyber Coalition exercises and the work of the NATO CCDCOE) (Olmstead, 2024; Gray, et al., 2021; NATO, 2023).

The integration of AI into NATO's logistics not only increases operational efficiency but also serves as a critical component of its overall strategic posture. By enabling predictive logistics, real-time threat mitigation, and rapid force projection, AI empowers NATO to maintain a decisive advantage over adversaries. (Reynolds, et al., 2024) The Alliance's investments and doctrinal adjustments today are setting the stage for logistics supporting high-intensity operations under the most complex multi-domain threat environments. NATO thus exemplifies how militaries can harness AI trends to optimise logistics, translating innovation into strategic advantage.

Section 3: AI usage in Ukraine's military logistics

Ukraine offers a unique and urgent example of how AI can rapidly adapt under combat pressure. It examines how Ukraine has deployed AI tools like Brave1, Delta, and uncrewed delivery systems to maintain agility and resilience. These real-world applications show what works - and where risks emerge - when AI meets battlefield realities. Ukraine's battlefield integration of AI similarly illustrates how theoretical concepts of automation, predictive analytics, and logistical agility are being adapted under actual combat conditions. Ukraine's case complements NATO's doctrinal ambitions by grounding AI's potential in practice, offering valuable insights for any future military that seeks to apply these technologies in actual conflict. While the primary aim here is to explore how AI supports operations in dynamic conflict environments, this section also continues to trace the key AI-driven trends identified earlier - thus contributing to the first research question.

The war in Ukraine presents a real-world testbed for AI-driven logistics under extreme circumstances. The country's experience demonstrates why embracing AI in military sustainment matters: facing a larger adversary, Ukraine has had to fight smarter and leverage technology to keep its army supplied, agile, and resilient. In a conflict defined by rapidly shifting frontlines and relentless attrition, AI-based logistics solutions have helped Ukraine improve everything from equipment uptime to the speed of ammunition resupply. Ukraine – and Kyiv in particular – has a strong potential to become a European leader across several applications of AI (United Nations Industrial Development Organisation (UNIDO), 2024). Understanding Ukraine's battlefield innovations provides valuable lessons in how AI can enhance future military operations and underscores the urgency for modern militaries to adapt. (Goncharuk, 2024)

The evolution of conflict in Ukraine from conventional warfare to hybrid operations - which combine kinetic engagements with cyber and information warfare - has necessitated a radical shift in logistical strategy. This integration of predictive analytics with real-time decision-making enhanced situational awareness and operational agility, providing commanders a decisive edge in adapting to rapidly changing battlefield conditions (McGee-Abe, 2023). In such scenarios, AI transforms logistics from a reactive function into a strategic asset that bolsters overall mission effectiveness.

Recent innovations and concrete examples that illustrate how AI has been applied in the field are such as the Avenger AI engine, the Brave1 project, Griselda, the integration with Delta, SmartLines, AtlasUAVs, and the integration of Starlink AI and Maxar Technologies. These validate the theoretical arguments and provide empirical evidence to support the claim that AI transforms logistics operations.

AI optimising trends enhance military operations in rapidly evolving conflict environments:

1. <u>Predictive analytics:</u> Ukrainian forces have implemented the Delta system - a digital command-and-control platform integrating real-time situational data - and Griselda. This AI-based platform processes extensive datasets from diverse sources to deliver real-time logistical predictions. This capability enables military commanders to dynamically adjust supply routes and resource allocation, ensuring that units receive essential materials promptly (Bondar, 2024). These predictive tools are complemented by the U.S. Army's Condition-Based Maintenance Plus (CBM+ (PANDA)), which continuously monitors equipment performance. By predicting malfunctions before they occur, CBM+ significantly reduces equipment downtime and alleviates the logistical burden during sustained military engagements (Mitchell, 2023).
2. <u>Autonomous systems:</u> Platforms such as Milrem Robotics' THeMIS - an uncrewed ground vehicle (UGV) for casualty evacuation and resupply - and Boston Dynamics' robot dogs exemplify how uncrewed systems can operate in hazardous combat environments, reducing human personnel risks while ensuring continuous supply chain operations. AtlasPro UAVs have been deployed to deliver ammunition, medical supplies, and food directly to frontline units. (Samus, et al., 2025; Defencemirror.com bureau, 2025; Army Recognition Group, 2022) Additionally, the extensive use of drone technology, particularly first-person view (FPV) drones equipped with automated target recognition, has enhanced resource allocation and battlefield surveillance. These drones provide real-time high-definition imagery and analytics, which facilitate precise logistical manoeuvres even in rapidly evolving conflict zones (Army Recognition Group, 2024; Ukrinform, 2024; Militarnyi, 2024)

3. <u>Situational awareness:</u> The Avenger AI engine is a state-of-the-art analytical tool designed to process and analyse massive volumes of battlefield data in real-time. Developed through collaborations between military research institutions and technology firms, Avenger uses advanced machine learning algorithms to rapidly assess logistical needs, predict supply shortages, and identify emerging threats. Early evaluations in several NATO-aligned operations indicate that Avenger enhances operational responsiveness and logistical efficiency, thereby streamlining resource distribution and strategic planning (Тарасовський, 2024). In parallel, the Brave1 platform - a Ukrainian defence tech accelerator fostering military-civilian innovation - has emerged as a comprehensive solution for coordinating supply chains across dispersed military units. By integrating data from ground sensors, aerial reconnaissance, and satellite imagery, Brave1 creates a unified operational picture that facilitates the synchronisation of logistical efforts. This platform not only improves the flow of supplies but also enhances the strategic agility of Ukrainian forces by enabling swift adaptations to the fluid dynamics of hybrid warfare. The practical implementation of Brave1 reinforces the critical role of AI in modernising military logistics and underscores its potential to redefine operational practices in complex conflict scenarios (Fedorov, 2025; Tech Ukraine, 2023).

While the benefits of AI in logistics are substantial, they come with significant cybersecurity challenges. Securing AI systems is essential, especially regarding cyber warfare. Adversaries may exploit weaknesses to disrupt operations or alter results. The interconnected nature of AI-enhanced logistical systems exposes them to sophisticated cyber threats that could compromise operational integrity. In response, military organisations have increasingly adopted advanced cybersecurity measures. Blockchain technology, for instance, has been employed to secure logistics data, while NATO-supported initiatives have focused on developing secure cloud computing environments and AI-based threat detection systems (Chunawala, et al., 2024; NATO, 2024; NATO, 2024). Moreover, the secure integration of AI in drone warfare - ensuring the integrity of data transmission and robust target identification - illustrates the dual importance of operational effectiveness and cyber resilience (Тарасовський, 2024).

Implementing AI in Ukraine's military operations presents ethical and technical challenges despite its advantages. Concerns include algorithmic bias, data security, and potential exploitation, highlighting the necessity for strong control procedures. AI systems' efficacy is contingent upon the data quality utilised for training. Biased or inadequate datasets may result in inaccurate decision-making, compromising missions or endangering lives.

Ukraine has adopted AI as an essential instrument to tackle the complex difficulties arising from the ongoing conflict. AI applications within the Ukrainian military encompass logistics optimisation, predictive maintenance, and battlefield intelligence. For 2025, the strategic priorities for the Ukrainian military are the evolution of AI-driven drones and the resilience to possible disruption in supply chains. These advances enhance operating efficiency, allowing Ukraine to adjust to a rapidly changing military environment. (Kushnerska, 2025; Cushman, 2025; Cowan, 2025)

In summary, Ukraine's adoption of AI-driven military logistics exemplifies the transformative impact of technology on modern warfare. Through the strategic implementation of AI across various platforms, Ukraine has enhanced its operational efficiency, improved battlefield awareness, and strengthened its defence posture against adversarial threats. Advances in predictive analytics, autonomous platforms, and cybersecurity have collectively enhanced logistical precision, operational agility, and overall mission effectiveness. Innovations such as the Avenger AI engine and the Brave1 platform further exemplify the potential of AI to streamline supply chains and improve strategic planning. As NATO and allied forces continue to invest in these technologies, the fusion of human expertise with machine intelligence will be essential for ensuring that military logistics remain adaptive, resilient, and capable of meeting the challenges of future conflicts (Goncharuk, 2024; Samus, et al., 2025)

Section 4: Foresee: Challenges and prospects for AI in military logistics

This final analytical section focuses on the third research question. Building on the NATO and Ukraine case studies, it explores systemic risks such as cyber vulnerability, ethical dilemmas, and organisational inertia. It also considers emerging technologies like quantum computing, blockchain, and AI-targeting drones. This section is critical for understanding the long-term feasibility of AI logistics - as isolated tools and as part of resilient, adaptive ecosystems capable of supporting military effectiveness in complex future warfare environments.

Societies and economies will become increasingly automated and AI dependent (Ministry of Defence, 2024; Elsner, et al., 2025). The more integral and pervasive a domain is - especially as vital as military logistics - the higher its likelihood of being attacked or rigorously tested by adversaries. This reality necessitates a robust, alliance-wide approach to cybersecurity and the continuous development (dual-use) of advanced technologies such as AI and quantum computing to protect these essential systems. It also needs legislation that enables cooperation and collaboration (nationally and internationally).

Cyber threats are not exceptional in the modern digital battlefield - they are routine. Critical systems, especially those involved in logistics and supply chain management, are attractive targets for adversaries. The more these systems work, the more they become integral to military operations and, consequently, the more likely they will be scrutinised, attacked, or probed by hostile actors. Securing AI-driven logistics systems requires more than deploying advanced technologies; it necessitates a holistic approach that includes robust cybersecurity protocols, continuous system updates, and adopting complementary technologies like blockchain. NATO's approach, for instance, involves joint cyber defence initiatives, regular system audits, and standardised protocols to ensure interoperability. These strategies are essential for mitigating vulnerabilities and ensuring that AI integration supports, rather than compromises, operational continuity. (Olmstead, 2024; Richard, et al., 2024)

Cybersecurity translates into an operational environment where every networked system must assume constant vulnerability. For example, AI-driven logistics platforms that streamline inventory management, route optimisation, and predictive maintenance heavily rely on continuous data exchange and digital connectivity. As such, they present multiple points of entry for cyber intrusions. Empirical evidence from Ukraine's conflict demonstrates that adversaries often launch cyber offensives aimed at disrupting supply chains or testing the resilience of these digital infrastructures (Richard, et al., 2024). The reality is stark: regular red-teaming of AI systems, encryption of data feeds (potentially using quantum-resistant methods), and use of blockchain for data integrity are among the measures needed (Goncharuk, 2024). To address these risks, NATO's revised AI Strategy emphasises protecting and monitoring AI technologies as a top priority (NATO, 2024). In essence, as logistics goes digital, digital security becomes logistics security.

Secure integration also demands grappling with data quality, bias, and sharing issues. Logistics data (maintenance records, consumption rates, transport times) can be vast but complex to understand, coming from different nations, services, or legacy systems. NATO, for instance, faces the challenge of ensuring that allies' systems talk to each other (Reynolds, et al., 2024). NATO doctrinal updates will likely stress common data frameworks; establishing common data standards and taxonomies for military logistics is critical. Ukraine's reforms include creating an integrated logistics management system for all services, ensuring everyone "speaks AI" in a unified way. Soon, logistics officers might need as much data management expertise as supply management.

Additionally, biases or gaps in data can lead AI systems to draw wrong conclusions. If an AI has primarily peacetime data, it can miscalculate needs in wartime - this has been acknowledged: early versions of a U.S. AI maintenance tool underperformed in combat exercises because the training data lacked examples of high-intensity usage, leading to underestimation of parts needs. Thus, continuous retraining with relevant wartime datasets, simulation scenarios, and cross-validation is needed to make AI logistics reliable (Gray, et al., 2021).

The use of autonomous decision-making systems in logistics raises significant ethical concerns. For example, automated resource allocation may lack the human judgment necessary to address complex ethical dilemmas, while biases in training data can lead to unfair or suboptimal outcomes. These challenges underscore the need for comprehensive governance frameworks that establish clear lines of accountability and maintain ethical standards. Studies have recommended regular audits and rigorous testing protocols to mitigate these risks and safeguard against the dehumanisation of warfare (Bellaby, 2024; Szenes, 2023). NATO's principles of responsible AI use demand traceability and human judgement in AI decisions (NATO, 2024), which implies that AI-driven logistics must have precise human override mechanisms and audit trails (Gray, et al., 2021). Furthermore, organisational adaptation is challenging - militaries must recruit or train personnel with AI and data science skills and possibly create new structures to manage these systems (Goncharuk, 2024).

The bottom line is that the human dimension cannot be ignored. Technology might drive change, but ultimately, humans must guide how AI is employed, and they must trust it. Building that trust will require clear policies, leadership endorsement, and evidence that AI helps rather than undermines the mission.

AI's rapid evolution is reshaping the future of warfare, driving innovation in combat strategies, operational efficiency, and decision-making (Scharre, 2023). A notable advancement is the integration of quantum computing, which enables real-time simulation of complex battlefield scenarios, enhancing strategic planning under pressure. As a frontrunner in military AI adoption, Ukraine exemplifies how such technologies can adapt to the demands of modern conflict. Increased deployment of uncrewed ground vehicles and AI-targeting drones is anticipated, reinforcing Ukraine's focus on precision, protection, and technological superiority in logistics and combat operations (Balmforth, 2024; Defencemirror.com bureau, 2025).

From quantum computing and autonomous systems to cyber defence and augmented reality, the innovations on the horizon have the power to reshape the battlefield. By addressing ethical concerns and fostering international collaboration, Ukraine can pave the way for a future where AI enhances security, efficiency, and strategic decision-making.

Conclusion and Recommendations

Conclusion

This study finds that integrating AI technologies - such as predictive analytics, autonomous systems, and cybersecurity - signals a paradigm shift in military logistics, comparable in scope to the earlier mechanisation of warfare, as illustrated in Table 1. One of the most significant developments observed is the strategic transition from human control to algorithmic coordination. NATO's doctrinal planning and Ukraine's real-time applications demonstrate how logistics is evolving from human-directed supply operations to systems increasingly managed by AI-driven decision-making tools. This transformation reflects a more profound rethinking of sustainment as a dynamic, autonomous process - enhancing speed, precision, and resilience in high-intensity conflict environments. Thus, AI does not merely support logistics - it redefines its role within military operations.

Drawing on insights from Ukraine's battlefield innovations and NATO's strategic initiatives, this study finds that AI is already reshaping military logistics and holds even more significant potential for future conflicts. Three primary conclusions answer the research questions posed at the outset:

1. Key AI trends in military logistics**:** The research mapped various technological developments that exemplify how AI optimises sustainment operations across different levels of warfare. Modern militaries leverage AI to optimise logistics through several prominent trends. Predictive analytics and maintenance systems forecast supply needs and pre-empt equipment failures, increasing readiness and efficiency. Autonomous platforms and robotics are carrying out supply deliveries and reconnaissance, reducing risk to human personnel and ensuring sustainment in contested areas. Advanced data integration and decision-support tools give commanders real-time visibility over complex supply chains. These trends were evident in NATO's forward-leaning logistics programs and in Ukraine's wartime adaptations, all aimed at making military supply systems faster, more precise, and more resilient.
2. Enhancing operations in rapidly evolving conflicts: The case of Ukraine demonstrated how these AI-driven trends enhance operational agility and resilience in rapidly evolving combat environments, allowing for faster decision-making and more precise logistical manoeuvres. AI allows forces to respond to changing battlefield conditions with agility by speeding up decision-making and delivery. For example, predictive logistics algorithms, autonomous supply drones and vehicles ensured that essential parts, ammunition and medical supplies reached forward positions in Ukraine to sustain combat power. AI-enhanced logistics also improved situational awareness – commanders could anticipate when and where resources would be needed based on AI forecasts and thus were better prepared for surprise developments. Collectively, these capabilities mean that an army employing AI-optimised logistics can outpace an adversary. The Ukrainian case, where a smaller nation held off a larger adversary with the help of tech innovations, underscores that AI logistics can be

a force multiplier, boosting operational tempo, reducing downtime for equipment, and ultimately increasing combat effectiveness in rapidly evolving conflicts.

3. Secure integration of AI-driven logistics: The analysis of both NATO and Ukraine revealed several key risks that must be addressed to securely and effectively embed AI into military logistics at scale. Cybersecurity and data integrity are the main concerns: AI logistics systems could fail at critical moments or work against the user. Robust cyber defences – such as encrypted communication channels, blockchain-backed databases for supply chain transactions, and continuous network monitoring – are needed to secure these AI tools.

   Additionally, the interoperability of systems is essential for secure integration. NATO's efforts in standardising data formats and interfaces for logistics AI ensure that allied nations can securely share information. Another aspect is ethical and organisational readiness: militaries must establish clear policies on AI use and train their personnel accordingly. AI-driven logistics can be securely embedded into military operations by instituting strong cybersecurity measures, ensuring systems can work together across units and allies, and maintaining human-in-the-loop oversight to handle complex or sensitive decisions.

   NATO's ongoing AI investments reflect a strategic push to embed these technologies into key doctrines such as AJP 3.4A (Allied Joint Doctrine for Non-Article 5 Crisis Response Operations) and AJP 3.20 (Allied Joint Doctrine for Cyberspace Operations). This integration addresses current logistical challenges while enhancing adaptability to emerging threats in modern warfare.

In conclusion, AI's current and near-future impact on warfare logistics is profound. AI technologies are streamlining military supply chains and maintenance, enhancing combat endurance and agility (as shown in Ukraine). At the same time, the full realisation of AI's benefits will depend on addressing the vulnerabilities of digital transformation. Militaries investing in innovation and protection – advancing their AI capabilities while fortifying them against threats – will likely gain a significant strategic advantage in modern warfare.

Recommendations

NATO–Ukraine collaboration on AI in logistics is already remarkable, with joint investments in advanced R&D areas like quantum computing, swarm intelligence, and energy-efficient systems. However, continued efforts are needed to maintain technological leadership and address warfare's most demanding supply chain challenges.

To enhance cybersecurity and data integrity, Ukraine must adopt strong cybersecurity protocols, utilise AI-powered cyber defence mechanisms, and create interoperability standards with allied nations. Clear policies need to define the scope of autonomous decision-making in logistics systems versus the necessity for human approval, ensuring alignment with ethical standards and international laws of armed conflict.

By developing specialised training programs for military logisticians and technicians and promoting a culture of multidisciplinary collaboration, armed forces can strengthen the human component of AI systems while enhancing familiarity, trust, and the capacity to address complex technological and ethical challenges.

Abbreviations

AI – Artificial Intelligence

ALIS - Autonomic Logistics Information System

CBM+ - Condition-Based Maintenance Plus

CCDCOE - NATO Cooperative Cyber Defence Centre of Excellence

DIANA - Defence Innovation Accelerator for the North Atlantic

NATO – The North Atlantic Treaty Organisation

ODIN - Operational Data Integrated Network

PANDA – Predictive Analytics and Decision Assistant

R&D – Research and Development

RMA - Revolution in Military Affairs

UAV - Uncrewed Aerial Vehicle

UGV - uncrewed ground vehicle

UNIDO - United Nations Industrial Development Organisation

References

Army Recognition Group. 2024. *Latvia Sends Over 500 Drones to Ukraine as Part of International Drone Coalition.* s.l. : Global Defence News - Army Recognition Group, 2024.

—. 2022. *Milrem Robotics delivers THeMIS CASEVAC medical evacuation UGV to Ukraine.* s.l. : Global Defence News - Army Recognition Group, 2022.

Balmforth, Tom. 2024. Ukraine sees use of uncrewed ground vehicles, AI-targeting drones surging next year. *Reuters.* 2024.

Bellaby, Ross. 2024. The ethical problems of 'intelligence–AI'. *International Affairs.* 2024, Vol. 100, 6.

Bondar, Kateryna. 2024. *Understanding the Military AI Ecosystem of Ukraine.* s.l. : Center for Strategic & International Studies (CSIS), 2024.

Chunawala, H. and Chunawala, P. 2024. Enhancing Cybersecurity in Cloud Environments Using AI-Driven Threat Detection and Response. *International Journal of Futuristic Innovation in Engineering, Science and Technology (IJFIEST).* 2024.

Cowan, Gerrard. 2025. Feature: NATO's DIANA plans to double innovation competitions, seeking dual-use advantages. *Janes.* 2025.

Cushman, Jeremiah. 2025. Supply chain modernisation key to future fight. *Janes.* 2025.

Defencemirror.com bureau. 2025. *Ukraine to Deploy Robotic Dog Units on Frontline.* s.l. : DefenceMirror.com, 2025.

Eisenhardt, Kathleen M. 1989. Agency Theory: An Assessment and Review. *The Academy of Management Review.* 1989, Vol. 14, 1, pp. pp. 57-74.

Elsner, Mark, Atkinson, Grace and Zahidi, Saadia. 2025. *Global Risks Report 2025.* s.l. : World Economic Forum, 2025.

Erbel, Mark and Kinsey, C. 2015. Think again – supplying war: reappraising military logistics and its centrality to strategy and war. *Journal of Strategic Studies.* 2015, 41(4).

F-35 Joint Program Office. 2022. *F-35 Joint Program Office completes initial deployment of new, improved logistics hardware.* s.l. : Eglin Air Force Base , 2022.

Fedorov, Mykhailo. 2025. How Brave1 contributes to the development of Ukrainian defense tech. *The Odessa Journal.* 2025.

Gilli, Andrea, Gilli, Mauro and Grgić, Gorana. 2025. NATO, multi-domain operations and the future of the Atlantic Alliance. 2025, 44 (1).

Goncharuk, Vitaliy. 2024. *Russia's War in Ukraine: Artificial Intelligence in Defence of Ukraine.* s.l. : ICDS, 2024.

—. 2024. Survival of the Smartest? Defense AI in Ukraine. [book auth.] Heiko Borchert, Torben Schütz and Joseph Verbovszky. *The Very Long Game: 25 Case Studies on the Global State of Defense AI.* s.l. : Springer, 2024.

Gray, Maggie and Ertan, Amy. 2021. *Artificial Intelligence and Autonomy in the Military: An Overview of NATO Member States' Strategies and Deployment.* Tallinn : CCDCOE (NATO Cooperative Cyber Defence Centre of Excellence), 2021.

Johnson, James. 2020. Artificial Intelligence, Drone Swarming and Escalation Risks in Future Warfare. *RUSI Journal.* 2020.

Kudzko, Alena and Macko, Pavel. 2023. *The future of digital deterrence in Central and Eastern Europe.* s.l. : GLOBSEC, 2023.

Kushnerska, Nataliia. 2025. *Missiles, AI, and drone swarms: Ukraine's 2025 defense tech priorities.* s.l. : Atlantic Council, 2025.

Layton, Peter. 2021. *Fighting Artificial Intelligence Battles: Operational Concepts for Future AI-Enabled Wars.* Canberra : Joint Studies Paper Series; Department of Defense, 2021. Vol. No. 4.

Lobariev, Vadym. 2024. Similarities and Differences Between the Industrial Revolution and the Age of AI. *LinkedIn Corporation Web site.* [Online] February 16, 2024. [Cited: February 23, 2025.] https://www.linkedin.com/pulse/similarities-differences-between-industrial-age-ai-vadym-lobariev-lqw6c/.

Losey, Stephen. 2022. Pentagon completes first phase in replacing troubled F-35 logistics system. *Defense News.* 2022.

McGee-Abe, Jason. 2023. *One year on: 10 technologies used in the war in Ukraine.* s.l. : Tech Informed, 2023.

Militarnyi. 2024. *Українська компанія створила систему автоматичного розпізнавання та наведення БПЛА.* s.l. : «Ukrainian Military Center» Public Organisation, 2024.

Ministry of Defence. 2024. *Global Strategic Trends Out to 2055 (Seventh Edition).* s.l. : Ministry of Defence (UK), 2024.

Mitchell, Billy. 2023. *Air Force selects AI-enabled predictive maintenance program as system of record.* s.l. : Defensescoop, 2023.

NATO. 2024. Deterrence and defence. *North Atlantic Treaty Organisation Web site.* [Online] 2024. [Cited: March 22, 2025.] https://www.nato.int/cps/en/natohq/topics_133127.htm?selectedLocale=en.

—. 2021. DIANA: Defence Innovation Accelerator for the North Atlantic. [Online] 2021. [Cited: March 22, 2024.] https://www.diana.nato.int/.

—. 2024. Funding NATO. *North Atlantic Treaty Organisation Web site.* [Online] 2024. [Cited: 03 22, 2025.] https://www.nato.int/cps/en/natohq/topics_67655.htm.

—. 2024. *NATO Digital Backbone.* s.l. : North Atlantic Treaty Organisation, 2024.

—. 2023. *NATO's flagship cyber exercise concludes in Estonia.* s.l. : North Atlantic Treaty Organisation Web site, 2023.

—. 2024. *Official text: Summary of NATO's revised Artificial Intelligence (AI) strategy.* s.l. : NATO, 2024.

Olmstead, Mark. 2024. Into the Gray Zone: NATO Deterrence in a Graying and Multipolar World. [Online] 06 23, 2024. [Cited: 03 20, 2025.] https://thesis.unipd.it/retrieve/20b777ae-b87f-4590-85f4-0a2a8b8c13f3.

Osinga, Frans and Tim, Sweijs. 2021. *NL ARMS Netherlands Annual Review of Military Studies 2020: Deterrence in the 21st Century—Insights from Theory and Practice.* Berlin : T.M.C. ASSER PRESS, 2021. ISBN 978-94-6265-418-1.

Rashid, Adib Bin, et al. 2023. Artificial Intelligence in the Military: An Overview of the Capabilities, Applications, and Challenges. [ed.] Yu-an Tan. *Hindawi, International Journal of Intelligent Systems.* 2023, Vol. 2023, Article ID 8676366.

Raska, Michael. 2020. The sixth RMA wave: Disruption in Military Affairs? *Journal of Strategic Studies.* 2020, Vol. 44(4).

Reynolds, Ian and Atalan, Yasir. 2024. *Calibrating NATO's Vision of AI-Enabled Decision Support.* Washington : Center for Strategic & International Studies, 2024.

Richard, William and Akram, Waseem khan. 2024. Big Data's Role in Supply Chain Optimisation: Enhancing E-commerce with Scalable Data Storage and Future-Proof Cyber Defense Strategies. *Research Gate.* 2024.

Rogers, Everett M. 2003. *Diffusion of Innovations, 5th Edition.* New York : Free Press, 2003. ISBN 0-7432-5823-1.

Samus, Mykhailo and Artemenko, Oleksandra. 2025. The Impact of Artificial Intelligence in the Drones' War in Ukraine. 2025.

Scharre, Paul. 2023. *Four battlegrounds – power in the age of artificial intelligence.* New York : W. W. Norton & Company, 2023. ISBN 978-0-393-86686--5.

Stanley-Lockman, Zoe. 2019. Revisiting the Revolution in Military Logistics: Technological Enablers Twenty Years on. [book auth.] Margaret E. Kosal. *Disruptive and Game Changing Technologies in Modern Warfare.* s.l. : Springer, Cham, 2019.

Szabadföldi, István. 2021. Artificial Intelligence in Military Application – Opportunities and Challenges. *Sciendo; Land Forces Academy Review.* 2021, Vol. Vol. XXVI, No. 2(102).

Szenes, Zoltan. 2023. Reinforcing deterrence: assessing NATO's 2022 Strategic Concept. *Defense & Security Analysis.* 2023, Vol. 39, 4.

Tech Ukraine. 2023. *BRAVE1 — Ukrainian Defence Tech Cluster launch.* s.l. : Tech Ukraine, 2023.

Trofymenko, Olena, et al. 2024. Artificial intelligence applications in military logistic. *Systems and Technologies.* 2024, Vol. 5, No. 154.

Ukrinform. 2024. *Мадяр: Ефективність використання FPV-дронів у ЗСУ і в росіян - 20-40%.* s.l. : Ukrinform, 2024.

United Nations Industrial Development Organisation (UNIDO). 2024. *Mapping the use of artificial intelligence in priority sectors and the competitiveness of Ukraine.* s.l. : UNIDO, 2024.

Wakefield, Scott. 2021. *Leader–Follower vehicles to offer Army increased operational capability.* s.l. : U.S. Army, 2021.

Wilner, Alex and Babb, Casey. 2021. New Technologies and Deterrence: Artificial Intelligence and Adversarial Behaviour. [book auth.] Frans Osinga and Tim Sweijs. *NL ARMS Netherlands Annual Review of Military Studies 2020: Deterrence in the 21st Century—Insights from Theory and Practice.* The Hague : T.M.C. ASSER PRESS;, 2021.

Zaluzhnyi, Valerii. 2023. Modern Positional Warfare and How to Win in It. *The Economist.* 2023.

Тарасовський, Юрій [Tarasovskyi, Yurii]. 2024. Сили оборони виявляють 12 000 цілей щотижня завдяки штучному інтелекту – Міноборони [Defence Forces detect

12,000 targets a week thanks to artificial intelligence - Ministry of Defence]. *Forbes Ukraine.* 2024.

BEST ESSAY OF THE HIGHER COMMAND STUDIES COURSE (HCSC)

LTC Linas Idzelis. Preparing for resistance in Lithuania. Implementation of historical and contemporary lessons to prepare for resistance to invasion and occupation

Introduction

Sooner the iron will turn into wax
and water into stone
than we disown the word we have spoken
– Gediminas, Grand Duke of Lithuania

After Russia illegally annexed Crimea in 2014 and started a full-scale invasion into Ukraine in 2022, there were many debates among military leadership in Lithuania whether or not national resistance has future in the contemporary conflict with the potential aggressor. From a philosophical perspective, resistance is based on the hope that nothing is in vain and that your country will be liberated sooner or later. Even if the country is oppressed by external power, the resistance movement usually increases the morale component and spirit of citizens and the remaining national armed forces to continue the fight and wait for friendly forces to come forcefully and dislodge the enemy forces and subsequently restore independence. For the military planners, the resistance adds additional layer of deterrence into national defence planning, meaning that the existence of this organization cannot be secret in order for it to possess its deterrence value (Fiala, 2022).

Lithuania's national security is affected by negative global security developments, which have been very significant in recent years. Russia's ongoing war against Ukraine, seeking to change the global security architecture – all these processes are highly dynamic. These dynamics also pose challenges for Lithuania as a small country bordering Russia and its ally Belarus (VSD, 2024). To counter emerging threats from Russia and its allies, NATO has developed new graduated regional defence plans.

However, the Munich Security Conference, held in February 2025, clearly demonstrates that security in Europe is deteriorating and remains unpredictable in due course. With this in mind, planning and preparation for the national resistance is of paramount importance.

Thesis: While Lithuania is strengthening its capabilities to counter the potential adversaries by preparing for all possible contingencies, including resistance, it should take into consideration the experience of Ukrainian resistance movement as well as resilience building in the temporarily occupied territories. These lessons learned should lead to amended legislation, revised training programs and cooperation with partners that helps prepare to function in a common battlespace.

The research paper is written from Lithuanian perspective as a small NATO country with minimal strategic depth. Arguably, this paper focuses mainly on resilience building to prepare nation and contributes into overall resistance capability building and stresses that both resilience and resistance is not purely military business, but all country and every citizen should contribute into the planning and execution.

Besides that, the research paper considers that Lithuanian population is resilient to the hostile propaganda and narratives and will to resist due to the external events gradually is mounting. Since 2014 different NATO conventional and special operation forces are already in place and contribute to the national resistance training and capacity building. This paper is divided into two chapters. The first chapter explains the implementation of historical and contemporary lessons from soviet fight the Lithuanian resistance in the post-war years (1944-1953) as well as an overview about Ukrainian resistance in the Temporary Occupied Territories in 2023-2024. The second chapter explains how Lithuania is building resilience and prepares for resistance to invasion and resistance to occupation. The paper ends with conclusions and recommendations from strategical to tactical level to improve the existing modus operandi and strengthen preparation to the national resistance.

1. Implementation of historical and contemporary lessons

Starting from the Napoleonic wars in the ninety's century and through appraisals in 1830-1831 and then in 1863-1864, the War for Independence in 1918-1921 following the resistance in 1944-1953, Lithuania managed to recruit and arm from 0.5 to 4 percent of the entire population. In comparison, in Belgium and Denmark, there was about 2.5 cents during the Second World War, and in France, from 1 to 3 per cent. The biggest amount members of the resistance movement was in Poland, calculated from 10 to 15 percent. Besides that, also important to know, that some population joint different oppressing organizations, such as KGB or in other means actively collaborated with occupies authorities (Jokubauskas, 2018). The survey conducted by Professor Ainė Ramonaitė in late 2023 asserts that around 30 percent of Lithuanians are ready to defend their country with weaponizing their hands, while 60 percent are ready to contribute to the defence in other ways. "The idea of total defence is ingrained in the consciousness of the Lithuanian people, and the majority of them are ready to contribute to the country's defence, with or without arms" (Ramonaitė, 2023). Although the numbers of the given survey are staggering, the real numbers of resistance movements can be clear only when an imminent threat occurs. To conclude, these numbers give an overview that when we are speaking about resistance, we cannot estimate that the whole society will resist in case of military confrontation or during the occupation.

Currently, the prevailing perspective among military leaders is that a resistance movement would serve as a last-resort effort to defend occupied territory in Lithuania. This aligns with the views of British Lieutenant Colonel Colin Gubbins, who suggested that resistance efforts could, in some cases, be short-term solution only until their resources are depleted or until members are captured or neutralized (Gubbins, 1939).

1.1. Soviet fight the Lithuanian resistance in the post-war years 1944-1953

In the summer of 1944, the Lithuanian Freedom Army, which had already been formed in 1941, began resistance after the invasion of the Lithuanian territory by the Soviet army. During 1944-1945, the Lithuanian Freedom Army managed to send and train about 300 partisans to Germany, who were parachuted back to Lithuania armed and equipped. According to the data provided, between July 1944 and November 1945, the partisans, who were called "bandits" by the Soviets, actively ambushed roads and planned mines and killed around 3,000 soldiers, army and internal army officers, communist party workers and activists. An amnesty was granted in June 1945. Partisans who confessed were guaranteed not to be prosecuted. The armed struggle against those who did not surrender continued, with military units and units formed from local communists being sent to the aid of law enforcement units like NKVD (then KGB, now FSB). Between July 1944 and November 1945, the Soviets carried out more than 9,000 operations, destroying 808 partizan units, hundreds of underground bunkers, a large number of food supplies, bases and weapons: 2,400 machine guns, 1,400 submachine guns, 20,000 assault rifles, about 3 million rounds of ammunition and a large number of grenades.

After the suppression of large partisan units, activities continued in small armed groups. Under these conditions, the main methods of struggle of the NKVD became: agent infiltration into the partisan underground, the use of alleged agent groups, the unmasking and splitting up of the nationalist underground, the organisation of Chekist-military operations (where necessary). Agent infiltration into the nationalist underground was carried out by recruiting agents from the most active members of the nationalist underground, by infiltrating into partisan units agents who had previously been transferred to an "illegal" position, and by planting agents of the NKVD organs in the ranks of the leaders of partisan units and organisations. The most effective way of infiltrating the nationalist underground was by recruiting agents from conspiratorially arrested bandits who had confessed to their crimes. They would agree to cooperate with the security organs. These agents were well known to the partisans, each of them was fully trusted and considered to be "their own" man, which allowed the security organs to use them immediately in active Chekist events. With the help of such agents, partisans' hiding places and routes of movement were identified, commanders, active participants and runners were identified, the role of each one, specific hostile activities and channels of communication with other partisan units and abroad were clarified, and the intentions of the partisans' hostile activities were known. The conditions were created for striking an operational blow ‘against the armed gangs by capturing the bandits’, and in particular the big leaders of the nationalist underground, alive. Agents were often dressed in the uniforms of officers of the formerly independent Lithuanian army, which were worn by many of the partisan members or combined with civilian clothes. This tactic proved to be very successful, and in the first four months of 1951 alone, with the help of the agent groups, 62 partisans were liquidated, including 25 leaders. Later, by 1953, a number of other participants in the armed resistance had been captured, including the commander of the resistance movement, Gen. Jonas Žemaitis. This proves that the tactics used by the Soviets had paid off and produced results (Vaigauskas, 1986).

1.2. Ukrainian resistance in the Temporarily Occupied Territories (TOT) 2023-2024

The Russians implemented their occupation plan in the areas that they seized. The FSB formed Temporary Operational Groups (TOGs), tasked with coordinating the occupation regime and its counterintelligence apparatus. Each TOG was assigned detachments of Rosgvardia for cordoning and public order, Alpha detachments and other special forces troops for conducting raids, and troops, including Chechen Rosgvardia detachments, intended to conduct the elimination of high-value targets. The TOG appointed a garrison commander from the Russian military within each town with an assigned detachment of garrison troops. These troops occupied a building – usually the police or fire station – and set up facilities for detention, processing, interrogation and torture. The fact that the layout of these facilities is consistent throughout the country, and the equipment used in torture chambers, including specialised electrocution machines, were the same across multiple oblasts demonstrates that this was a systematic plan and not an improvised sadism. The population was divided into five core categories:

1. Those deemed leaders of Ukrainian nationalism who were specified for physical liquidation on a high-priority target list.
2. Those suspected of intending to support acts of resistance who needed to be recruited or suppressed, including anyone associated with Ukrainian law enforcement, local government, the military or related to officials that were not actively collaborating.
3. Those who were deemed apathetic.
4. Those actively collaborating with Russian forces.

5. Individuals who were necessary for running critical national infrastructure and had to be controlled.

At the same time, garrisons were tasked with conducting house-to-house sweeps. This involved military units inspecting houses to confirm that the records seized accurately recorded who was at each address. They also searched homes for insignia, medals or uniforms indicating whether residents had previously had connections with the Ukrainian state and examined photographs and other personal effects to confirm the relationships between residents. First, for those on the high-priority target list identified as Ukrainian nationalists the intent was to kill or capture them – spearheaded by Chechen units and the FSB (RUSI, 2023).

The invading forces regularly conduct filtration activities, house-to-house visits, random checks on the street, and situationally deploy checkpoints around settlements where cases of underground activity are recorded. As a result, thousands of people (the exact number is unknown) are being held in camps on the TOT without official charges. In particular, the population suspected by the Russians of disloyalty is held in camps in Genichesk, Arabatska Strilka, and in a network of detention centres in the Autonomous Republic of Crimea, Donetsk and Luhansk regions. The enemy has also built a filtration camp in Chongar (Crimea) for these purposes (NRC, 2024).

Despite Russian very harsh imposed counter-intelligence regime, Ukrainians keep fighting with invading forces. According to the invaders, there are up to 5-7 thousand people on the TOT whom they suspect of involvement in underground movements. These include: "S.R.O.K." ("death to Russian invaders and collaborators"), resistance movements "Kakhovka movement", "Melitopol movement", "Berdiansk partisan army" and the Crimean Tatar resistance movement "ATESH", as well as the public movement of resistance to the occupation "Yellow Ribbon".

Below are specific examples and evidence supporting the claims regarding effective operations conducted by Ukrainian resistance movements in the TOT. These examples reflect different forms of resistance, such as sabotage, ambushes, and intelligence sharing and others.

- Railroad Sabotage: Ukrainian resistance groups have been known to target railway lines that supply Russian troops. For instance, in 2023, partisans reportedly derailed Russian military trains and disrupted logistical operations in the Zaporizhzhia region.

- Assassinations of Russian Officers: Ukrainian partisans have reportedly carried out successful assassinations of Russian commanders. For example, in June 2023, a senior Russian officer was killed in an ambush in the town of Melitopol.
- Ambushes on Russian Military Convoys: There have been numerous reports of ambushes carried out by local resistance forces. In 2023, Ukrainian partisans reportedly ambushed Russian convoys near the city of Kherson, causing casualties and damaging military vehicles.
- Improvised Explosive Devices (IEDs): Resistance groups in occupied areas have used IEDs extensively. These devices are often placed on roads, in vehicles, or near Russian military positions. One notable attack occurred in April 2023, when an IED exploded near a Russian military vehicle in the Donetsk region, killing several Russian soldiers.
- Intelligence Gathering: Ukrainian resistance groups have played a key role in providing intelligence to the Ukrainian armed forces. This includes identifying Russian troops movements and locations. For instance, local resistance in Mariupol and Kherson provided detailed information that led to successful Ukrainian counterattacks.
- Use of Drones: Resistance forces in occupied territories have used drones for reconnaissance and attacking Russian military positions. In 2023, Ukrainian partisans in occupied areas reportedly launched drone strikes on Russian fuel depots in the city of Melitopol, resulting in significant damage (AFU, 2025).

In conclusion, despite the systematic and oppressive measures implemented by the Russian forces to suppress dissent and maintain control, Ukrainian resistance movements have demonstrated remarkable resilience and adaptability. Through diverse tactics such as sabotage, ambushes, intelligence sharing, and the use of drones, these groups have not only disrupted the occupiers' operations but also maintained a spirit of defiance and hope among the population. Their efforts underscore the enduring struggle for sovereignty and the unyielding determination to reclaim their homeland.

2. Building the resilience capacity and preparing for resistance

Resilience is the foundation (see Figure 1) of resistance through which a state can regain national sovereignty and where resilience and resistance activities overlap (Fiala, 2020).

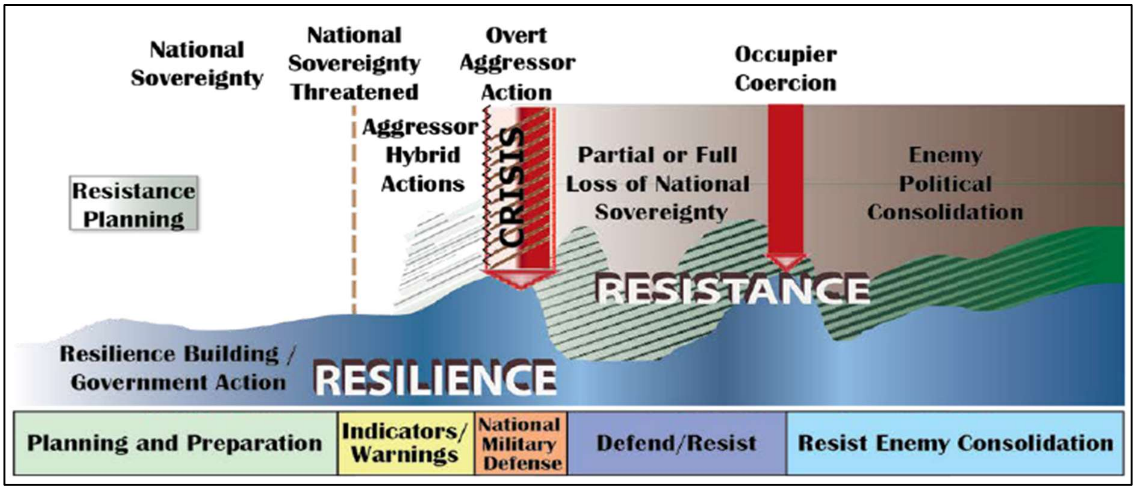

Figure 1. Resilience as the Foundation of Resolute Resistance in National Defence. Source: (Fiala, 2020)

Building the national resilience capacity is strongly recommended for all countries, especially neighbouring the potential aggressors. To meet the Resistance Operating Concept (ROC) requirements, resilience is described as the will and ability to withstand external pressure and influence and/or recover from the effects of those pressures or influence. To this end, national resiliency is enhanced by forming a national resistance capability to restore sovereignty. Resilience is thus distinguishable from resistance and is a necessary pre-condition for successful resistance operations. A highly resilient population can be created by developing a strong national identity and preparing to overcome crises, strengthening a nation’s will to resist. The government should communicate the existence of potential external threats to its own population, along with its plans for the population and military to counter or mitigate those threats through preparedness, training, and the necessary institutional and legal structures and policies (Fiala, 2020).

Building the national resilience capabilities is a government-monitored and long-lasting process. It includes Whole–of–society and Whole-of-government thinking, which discuss comprehensive state preparation at all possible levels.

2.1. Whole–of–society approach in modern Lithuanian society

To involve Lithuanian citizens in the defence architecture in 2022, the Parliament of the Republic of Lithuania approved the strategy for preparing citizens for civil resistance. The document includes consistent and comprehensive public education on civil resistance. Such preparations will rest on three components: civil resilience, will to resist, and practical skills in both, armed and civil resistance. Implementing the strategy, the Mobilisation and Civil Resistance Department under the MOD, with the support of the Lithuanian Riflemen's Union (LRU), have developed special civil-based resistance courses. The first level course gives a general overview for the participants on how the population can resist the aggressor as well as provide support to the Armed Forces of Lithuania. The second level course aims to describe the participants how Russia, with it's allies, is waging hybrid warfare also how to distinguish hostile soldiers and different armoured vehicles, airplanes, air defence systems etc. and then report to authorities.

A new course has just been established with the purpose of teaching the population how to prepare for evacuation, what to take and what to pack. Estimated to scale this course to the extent that every Lithuanian citizen would be trained on how to survive for at least three days being self-sustainable. Besides that, LRU, in 2022, started a three-day education campaign for ninth-grade pupils at secondary schools. During this intensive course, LRU instructors familiarise the audience with survival skills, weapons handling, aiming and land navigation.

After successful activities among Lithuanian MOD, LRU and the Ministry of Education last year, an agreement was signed to further work on this project and establish similar courses with different subjects at lower or higher grades (Respublika, 2024). Furthermore, LRU, after Lithuania regained independence, started cadet training. Currently, LRU trains annually about seven thousand cadets from eleven to eighteen years old with different military disciplines, leadership, and national patriotic pride in young people. Moreover, LRU, during the last few years, started forming different units abroad in the Lithuanian diaspora and plans to expand and establish a separate command responsible for training and exercises. To bring an example, the LRU unit in Benelux countries united Lithuanian citizens and funds were raised for first person drones, then organized a workshop, ‘Wings for Europe’, constructed dozens of pieces and sent them to Ukraine. This encouraging example illustrates the necessity of the diaspora and its involvement in civic activities (LRU, 2024).

Letting civilians prepare for the armed resistance and ensuring that everyone understands their roles, the Lithuanian Armed Forces in 2024 changed the structure of military commands in peacetime. It was announced in the mass media that all patriotic citizens can sign up. People of all specialties and backgrounds who wish to prepare for national defence and acquire basic military knowledge and skills were welcome in the commandant's offices. Citizens wishing to contribute to national defence and acquire military skills were encouraged to register at the nearest Military Conscription and Recruitment Centre (MCRC). Persons registered in the Command Units will be trained for 3-10 days per year, by being called up to participate in exercises as part of this unit, together with other members of the Ready Reserve scheduled for these units. In the event of war, citizens enrolled in the Command Units and trained in military skills will help to defend their town or district and to protect important objects in their living environment. Persons belonging to the units will take care of the protection of vital infrastructure in their town or district, set up and man road checkpoints, enforce curfew rules, participate in the process of requisitioning property, monitor the environment, fight against illegal armed groups, or carry out any other tasks assigned by the Lithuanian Armed Forces. To strengthen Command Units more than two thousand active members of the LRU were attached to this formation, who will organise and plan exercises (LAF, 2024).

2.2. Whole-of-government approach in modern Lithuanian society

Strengthening state resilience the Parliament of the Republic of Lithuania passed the Law on Mobilization and Training of Mobilization Reserve in late 1996, thus giving the legal basis for action on mobilisation professional supervision of preparation of ministerial, municipal institutions and agencies, economic entities and other bodies of the state for mobilisation, their contribution in preparation and delivery on host nation support objectives, implementation of mobilisation and demobilisation. To observe and control that all the above-mentioned organizations developed and updated their mobilization plans, established alternative command posts, as well as conducted regular exercises, the Mobilization and Civil Resistance Department (MCRD) under the MoD was established already in 1997 (MOD). Regularly, MCRD organises top table exercises in different Lithuanian regions and investigates whether participants are ready to transform their organisations from peace to war establishment if crises or war comes.

To coordinate inter-agency cooperation and provide early warning to the decision-makers when it is necessary, the National Crisis Management Centre (NCMC) under the Government has been established. NCMC manages crises and emergencies and operates on a 24/7 basis and continuously monitor the threats to Lithuania’s national security interests. In case of a crisis or an emergency, the NCMC will ensure the management of these situations and will also coordinate the prevention of national security threats and the activity of state reserve managers, as well as strategic communication about national security. The NCMC also is tasked to ensure the activities of a National Security Commission and coordinate the mobilisation of non-governmental organisations and volunteers at the national level. The centre also organises national and international-level crises and emergency management exercises (LRT, 2022).

Facilitating State Survivability in 2022, the Government of Lithuania approved six vital state functions and all ministers, municipal institutions and agencies, economic entities and other bodies of the state for mobilisation identified more than sixty thousand positions, which are mandatory to man in case of crisis or war, when others would be evacuated to the safe haven. All six vital six vital state functions are listed below:

1. National defence (this vital state function includes: armed defence; civil resistance; support of civil mobilisation institutions to the Armed Forces of the Republic of Lithuania; combating information threats; cyber security and cyber defence; provision of critical information infrastructure, state information resources, electronic communications services; intelligence and counter-intelligence).

2. State governance and the activities of municipal institutions (this vital state function includes: state governance (the activities of the President of the Republic of Lithuania, the Seimas of the Republic of Lithuania, the Government of the Republic of Lithuania, municipal institutions); the activities of the courts, the public prosecutor's office and penitentiary institutions; informing the public about the situation in the country; and the preservation of movable and immovable cultural property, documents and archives).
3. The functioning of the economy and the civil infrastructure (this vital function of the State includes the operation of the financial, energy and transport systems and the management of spent nuclear fuel and radioactive waste).
4. Meeting the basic needs of the population (this vital State function includes: the provision of personal and public health services; the provision of foodstuffs and potable water to the population; the detection of environmental pollution).
5. Internal security (this vital State function includes: ensuring public order and public security; operating the civil protection system).
6. International activities (this vital State function includes: continuity of the activities of the diplomatic missions and consular offices of the Republic of Lithuania abroad; ensuring the cooperation of the Republic of Lithuania with international organisations and foreign countries; possible organisation of the continuity of State governance in a foreign country (LRS, 2022).

The Government of Lithuania's detailed approach to defining and safeguarding vital state functions underscores its proactive stance in ensuring national resilience. These measures reflect not only a commitment to the protection of the nation's core systems and population but also a readiness to adapt and respond to modern challenges. Such strategic preparation serves as a robust foundation for preserving state sovereignty and continuity in the face of potential crises.

In the contemporary conflict, we can distinguish two potential methods for the resistance. They are as follows:

2.3. Resistance to invasion

Resistance to invasion refers to the effort to prevent or dislodge enemy forces from breaking in or advancing within a country. This type of resistance can range from direct military confrontation to nonviolent civil efforts. The main goal is to stop invaders and protect motherland from foreign control. It is associated with whole-of-government and whole-of-society approach. It constitutes that all ministries, municipalities and other governmental organizations convert from peace time into war time establishments. As concurrent actions all paramilitary organizations, low enforcement agencies, hunters, practical shouting associations, non-governmental organizations join total defence. Armed defence through conventional military methods is executed and at the same time the guerrilla warfare employing ambushes, raids and hit-and-run strategies is implemented. This type of resistance might be strengthen with diplomatic interventions for international aid or condemnation, as well as civil resistance such as protests and strikes. To avoid fratricide, all resistance movements within the country must be carefully coordinated by professional or reserve officers. This resistance method was recently observed when Russia invaded Ukraine, efforts included conventional military defence, civilian participation, and international diplomatic campaigns. After some territories became occupied by Russian military, initially involved military actions to resist invasion, focus shifted toward sabotage and guerrilla warfare which we can name as resistance to occupation.

2.4. Resistance to occupation

Resistance to occupation is usually a long-term struggle until the occupying force is driven out or the situation changes significantly (through negotiations, changes in the occupying power, or military intervention). Resistance to occupation starts when elements of friendly troops are overrun or defeated by enemy forces. According to the doctrine, denied area is an area under enemy or unfriendly control in which friendly forces cannot expect to operate successfully within existing operational constraints and force capabilities (3-05.1, 2016). On one hand, resistance to occupation involves actions taken against established foreign power’s control over a territory. It emphasizes undermining and weakening the occupier's influence and physical capabilities. Mainly executed using guerrilla tactics like sabotage, raids and ambushes.

On the other hand, this kind of resistance might not involve into direct actions to spare the resistance cels and fight when detected or ordered but provide valuable intelligence information to NATO partners for the deep strikes with loitering munition, drones and precision guided rockets (Ühtegi, 2025).

To sum up, while resistance to invasion and resistance to occupation may overlap in some aspects (especially when the invader seeks to occupy), they are distinct in their nature and strategies. Resistance to invasion is primarily defensive, seeking to prevent the enemy from establishing control, while resistance to occupation is more about undermining and destabilizing the occupying power once they've established a presence. Both methods might be included into countries defence plan as branch plan or separate annex.

Conclusions and Recommendations

In conclusion, the establishment of a resilient national defence framework, as outlined through the Lithuanian government's initiatives, highlights the critical role of resilience as a foundation for effective resistance against external threats. By fostering a comprehensive approach that integrates both Whole-of-Society and Whole-of-Government strategies, Lithuania has built a robust defence mechanism capable of withstanding and overcoming adversities. The proactive measures, including the implementation of civil resistance strategies, military preparedness programs, and inter-agency cooperation, empower not only the government and armed forces but also the civilian population to contribute actively to national defence.

The integration of civil society, as seen through initiatives like the civil resistance courses and the involvement of the Lithuanian Riflemen's Union, ensures that every citizen is equipped with the knowledge and skills to support national defence efforts, even in times of crisis. On the governmental front, the careful preparation of essential state functions ensures continuity and resilience across various sectors, from defence to healthcare and economic stability.

The findings suggest that resistance movements, whether in the form of preventing invasion or countering occupation, often rely on a mix of military tactics, guerrilla warfare, intelligence sharing, and civil disobedience. In both Lithuania's past and Ukraine's present, the involvement of the civilian population, combined with professional military support, strengthens the ability to resist and destabilize the occupiers. The resilience and adaptability shown by Ukrainian resistance groups in occupied territories—despite harsh repression and counterintelligence operations—illustrate the enduring power of national identity and the determination to reclaim sovereignty.

While the success of resistance depends on a range of factors, including the level of external support, internal unity, and the effectiveness of counterintelligence, it is clear that such movements can significantly disrupt occupiers and contribute to the eventual restoration of control. The Lithuanian and Ukrainian experiences serve as powerful reminders of the importance of collective defence, the complexities of resistance under occupation in the denied area, and the unyielding human spirit in the face of foreign oppression. Resistance, whether through armed struggle or nonviolent means, remains a vital tool in safeguarding a nation's independence and identity.

Recommendations

The analysis recommends and calls for action Lithuanian civil and military top leadership. Firstly, for Lithuanian Ministry of defence and Lithuanian Parliament National Security Council to amend and renew Law on National Security Framework and Law on Martial Law of the Republic of Lithuania. Thus, necessary to prepare and enable for resistance (caches of different weapons, ammunition, documents and etc.) in the peace time, as well as to define clear responsibilities among civilian and military organizations.

Secondly, for the Lithuanian Armed Forces Training and Doctrine Command to revise and amend Lithuanian Military Doctrine and clearly define the responsibilities of different actors in the resistance. Besides that, to specify the command and control during the defence and resistance phases. Furthermore, collect lessons identified from Russo – Ukraine war and issue handbook for leaders and potential resistance fighters.

Additionally, to include into all levels leaders training programs basics of the resistance organization and movement.

Thirdly, for the Lithuanian Rifle Union to establish close cooperation with the Ukrainian national resistance coordination unit and revise the training programs as well as organizational structure according to the needs of the contemporary battlefield.
Finally, a similar study should be conducted in all Eastern NATO flank countries to ensure preparation for the resistance and strengthen countries resilience. These actions would allow cooperating with likeminded countries and prepare as common battlespace.

Bibliography

VSD. 2024. The Defence Intelligence and Security Service (AOTD) and The State Security Department**.** *National Threat Assessment.* s.l. : Ministry of National Defence, 2024.

3-05.1, Joint Publication (JP). 2016. *Unconventional Warfare .* s.l. : United States Army Special Operations Command, fort Bragg, North Carolina, 2016.

AFU, SOF. 2025. Resistance Movement Experience (SOF AFU) in the Tasks of Combating the Full-Scale Invasion of the Russian Federation. Kyiv, Ukraine : s.n., 2025.

Fiala, C. Otto. 2020. *Resistance Operating Concept.* s.l. : The JSOU Press and Swedish Defence University, 2020.

—. 2022. Legitimazing the Resistance. *Journal on Baltic Security*. Vol. 8(1), pp. 151-170

Gubbins, Colin. 1939. *The art of guerilla warfare (And the partisan leader's handbook and general principles)*. s.l. : Printed in Great Britain by Amazon, 1939.

Jokubauskas, Vytautas. 2017-2018. Territorial Defence and Partisan Resistance (Lithuania's Experience). *Lithuanian Annual Strategic Review.* Vol. Volume 16.

LAF. 2024. Registration for military commands in peacetime opens. *Armed Forces of Lithuania.* [Online] Karys.lt, 2024. [Cited: 15 February 2025.] https://www.karys.lt/bendraukime/naujienos/pradedama-registracija-i-karo-komendanturas-taikos-metu/644.

LRS. 2022. Decision of Government of the Republic of Lithuania . *Approval of the list of vital State functions.* [Online] Parlament Republic of Lithuania, 2022. https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.426220/SGRvIbhJCf.

LRT. 2022. *Lithuania to establish National Crisis Management Centre.* [Online] 2022. [Cited: 16 February 2025.] https://www.lrt.lt/en/news-in-english/19/1854923/lithuania-to-establish-national-crisis-management-centre.

LRU. 2024. LRU members living abroad are invited to join the "Wings for Europe" project. *Lietuvos Šaulių Sąjunga.* [Online] 2024. [Cited: 15 February 2025.] https://www.sauliusajunga.lt/iseivijos-sauliai-kviecia-prisideti-prie-projekto-wings-for-europe/.

MOD. 2022. Ministry of Defence of The Republic of Lithuania. *Mobilization and Civil Resistance Department under the MoD.* [Online] 2022. [Cited: 16 February 2025.] https://kam.lt/en/mobilization-and-civil-resistance-department-under-the-mod-2/.

MOD. 2022. Lithuania, Ministry Of National Defence Republic of Lithuania. 2022**.** Seimas approves civil resistance readiness strategy. [Online] 2022. [Cited: 15 February 2025.] https://kam.lt/en/seimas-approves-civil-resistance-readiness-strategy/.

NRC. 2024. Situation in the TOT in the First Half of 2024. s.l. : National Resistance Centre, 2024.

Ramonaitė, Ainė. 2023. Professor of Vilnius University: 30 per cent of Lithuanians are ready to take part in the arm resitance. VU profesorė: 30 proc. lietuvių yra pasiryžę šalį ginti ginklu. *Made in Vilnius.* [Online] 2023. [Cited: 15 February 2025.] https://madeinvilnius.lt/naujienos/lietuvos-naujienos/vu-profesore-30-proc-lietuviu-yra-pasiryze-sali-ginti-ginklu/.

Respublika. 2024. Respublika . Kasčiūnas, who signed the tripartite agreement on the development of civic education, says military training of young people should be developed as early as possible. [Online] 2024. [Cited: 15 February 2025.] https://www.respublika.lt/lt/naujienos/lietuva/kitos-lietuvos-zinios/trisali-susitarima-del-pilietinio-ugdymo-pletros-pasirases-lkasciunas-karini-jaunimo-parengima-reikia-vystyti-kuo-anksciau/.

RUSI. 2023. Preliminary Lessons from Russia's Unconventional Operations during Russo-Ukrainian war, Feb 2022-Feb 2023. s.l. : Royal United Srvices Institute for Defence and Security Studies, 2023.

Ühtegi, Riho*. 2025.* Resistance Organization, Underground and Public Component. 2025**.** Tartu : BDCOL, 2025.

Vaigauskas, G.K. 1986. *Combating and countering the malign activities of Lithuanian nationalists.* Moscow : October Revolution, Order of the Red Flag F. Dzerzhinsky Higher School of the KGB, 1986.

LTC Nerijus Kačkauskas. The role of (strategic) leadership in developing resilience in military organizations

Introduction

The contemporary geopolitical landscape is characterized by precarious balances and fragile security, exacerbated by ongoing military conflicts and the heightened risk of new outbreaks. This poses significant challenges for the armed forces. Modern military personnel are highly skilled professionals who must operate effectively under demanding conditions. The rapid evolution of armed forces places increased pressure on soldiers and commanders to maintain exceptional performance, commitment, and well-being while ensuring high levels of duty fulfilment and service satisfaction. Therefore, overall, personal, organizational and state's ability to withstand challenges and risks and being resilient is crucial.

Resilience is a multifaceted concept that plays a critical role in various contexts, including *personal*, *state*, and *organizational* settings. 'Personally, resilience involves adapting to life's challenges, influenced by one's outlook and expectations. In organizations and societies, resilience is fostered by a shared purpose and principled leadership, which provide a sense of direction and unity' (Miniotaitė, 2022). 'From a state's perspective, resilience entails adapting to economic, environmental, and social challenges through a systems-thinking approach, enabling countries to absorb shocks and recover while maintaining operational continuity' (Howell, 2013). 'Organizational resilience refers to an organization's ability to anticipate, adapt, and recover from disruptions while maintaining operational continuity. It involves key dimensions such as robustness, agility, and adaptability, enabling organizations to manage crises effectively and transform challenges into opportunities for growth. Resilience is influenced by factors across individual, group, and organizational levels, including resources, routines, and adaptive capacities' (Xiao et al., 2017).

This paper examines how strategic leadership fosters resilience in military organisations, particularly emphasising the role of leaders' resilience as a foundational quality. Resilience is a crucial leadership quality, enabling leaders to recover from setbacks and maintain goal-oriented momentum. Leaders' resilience is assessed by their capacity to bounce back from mistakes, a trait that can inspire others to reframe failures as opportunities for growth. By adopting a resilient mindset, individuals can mitigate the perceived significance of mistakes and foster a more adaptive approach to challenges.

Therefore, this research paper claims that strategic leadership remains a fundamental pillar for building resilience in military organizations but identifies a significant knowledge gap in how the personal resilience of leaders can create a ripple effect to improve organizational resilience. Elaborating on this, the research investigates how strategic leaders cultivate a culture of resilience by employing personal resilience practices – such as adaptive decision-making under pressure and reframing setbacks as learning opportunities – and investigates how these practices can be systematically integrated into military organizational structures to enhance overall resilience. By bridging the individual and organizational dimensions of resilience, this research aims to demonstrate how strategic leaders' personal resilience practices can enhance military organizational resilience, addressing a critical gap in leadership development. The paper examines a broad spectrum of materials related to leadership development and resilience through empirical studies and academic reports alongside peer-reviewed papers, professional assessments, and trustworthy articles from esteemed publications. The study combines organizational psychology, strategic management, and military leadership research to examine resilience at both personal and organizational dimensions using interdisciplinary perspectives. The multifaceted approach enables extensive examination of theoretical frameworks and practical applications alongside evidence-based findings, which reveal how personal resilience in strategic leadership influences organizational dynamics, especially in military settings.

Leadership and its stance at strategic level

Military leaders enhance military competitiveness through competence and resilience, aligning tasks with training outcomes. Professional leadership development, grounded in national and organizational resilience, promotes a culture of personal responsibility and fosters professional growth within military forces. This chapter initially reflects leadership fundamentals, examines strategic level and its leadership qualities, their interconnections, and concluding with practical examples.

Understanding leadership

Leadership remains a highly valued asset, yet the characteristics of effective leadership remain a subject of ongoing inquiry. Extensive literature and military academies programs still see to define and cultivate skills that enhance organizational performance.

'Military leadership is a multifaceted construct that remains challenging to fully capture, with current approaches potentially falling short of providing a comprehensive understanding of leader capacity or effectiveness' (Nazri et al., 2019). 'Leadership research is increasing dramatically, and findings underscore that there is a wide variety of different theoretical approaches to explain the complexities of the leadership process. Some researchers conceptualize leadership as a trait or as a behavior, whereas others view leadership from an information-processing perspective or relational standpoint' (Northouse, 2022). Moreover, 'Leadership, along with discipline, ethics, organizational culture and specific socialization practices, is one of the most important pillars of the military profession. As such, professional military leadership is one of the key aspects emphasized at strategic level' (Codreanu, et al., 2022).

Leaders must equip themselves for complex challenges. While leadership resists rigid definitions, each leader interprets it uniquely. However, leadership is 'the process of developing individual and collective human and organizational capacity and providing the purpose, direction, and motivation required to employ that capacity to create effective and ethical combat power under intense, dynamic, and dangerous conditions […]' (Hannah, 2012).

Effective leadership is a dynamic process requiring fast, adaptive decision-making. The challenge for a leader is a timely response to situational changes and seeking favourable circumstances while at the same time dealing with risks. Because 'effective leadership is critical to military performance. Leaders who can inspire and motivate their troops, set clear goals, and provide guidance and support are more likely to foster high levels of performance' (Fernandes et al., 2024). Therefore, leadership remains an elusive art, driven by understanding human motivation to face risks.

How strategy influence strategic leadership?

Strategy can be understood as a concept and as a process. It is a generalized plan of action over a long period to achieve defined objectives. Merriam-Webster dictionary (2025) defines strategy as 'the science and art of employing the political, economic, psychological, and military forces of a nation or group of nations to afford the maximum support to adopted policies in peace or war'. Moreover, Halvorson (2025) emphasizes that 'strategy is where you will focus your efforts to achieve your goals, and how you will succeed or, 'where to play and how to win'. It defines a specific course of action that will take you from where you are now to where you want to be'.

Additionally, Henry Mintzberg (2024), as early as 1987, introduced the so-called 'The Mintzberg 5 Ps of strategy', which consists of concepts and approaches to strategy formulation that remain influential today. These include – *Plan* (a premeditated course of action), *Ploy* (manoeuvres to outmanoeuvre competitors), *Pattern* (historical organizational behaviour), *Position* (the organization's external standing), and *Perspective* (a shared vision guiding strategic decisions). This framework provides a comprehensive approach to strategy formulation by considering both internal and external factors. Therefore, strategy requires continuous effort, resulting in a plan to strengthen and expand organizational activities. 'The art of strategy allows the strategist to see the nature of the strategic environment and a path or multiple paths to his desired end-states; and the scientific aspect of strategy provides a disciplined methodology to describe the path in a rational expression of ends, ways, and means that shape the strategic environment in favorable terms' (Millen, 2012).

Furthermore, for the military, strategic level is the highest level of warfighting. APP-6 (2020) strategic level describes as 'the level at which a nation or group of nations determines national or multinational security objectives and deploys national, including military, resources to achieve them. Ibid, strategic concept described as the course of action accepted as a result of the estimate of the strategic situation. It is a statement of what is to be done in broad terms sufficiently flexible to permit its use in framing the military, diplomatic, economic, psychological and other measures which stem from it'. The strategic level covers national and international interests where policy plays a key role and it 'focuses on defining vision, mission, and objectives while managing resources' (Singleton, 2024). Nevertheless, that strategy encompasses both war and war preparation and plays a significant role during peacetime. Therefore, peacetime policymakers build the national vision, where military strategic level command draws its army's future vision. Thus, the relationship between strategic military and strategic political leadership is crucial. So, while formulating a strategy, clearly understanding concepts and establishing the correlation between *means*, *ways*, and *ends* is decisive. Therefore, and in the overall complexity of developing strategy and operating at a strategic level, organizations and leaders must focus on the organization's area of operation, where the organization operates (*strategic environment*), what tasks must be achieved (*strategic intent*), how it needs to be done (*strategic concept*) and specific goals (*strategic objectives*). Hence, the involvement of a strategic-level leader is crucial.

Thus, according to Guillot (2003), 'strategic leadership entails making decisions across different cultures, agencies, agendas, personalities, and desires. It requires the devising of plans that are feasible, desirable, and acceptable to one's organization and partners – whether joint, interagency, or multinational. Strategic leadership demands the ability to make sound, reasoned decisions – specifically, consequential decisions with grave implications'. Additionally, Guillot (2003) distinguishes between the aims of the strategic level and leadership, where he states that '[…] the aim of strategy is to link ends, ways, and means, the aim of strategic leadership is to determine the ends, choose the best ways, and apply the most effective means'.

A strategic leader looks at least 5 or 6 years ahead, unlike operational leaders handling short-term tasks. The main difference is that a strategic leader sets long-term goals and inspires people to work with him or her to achieve them, while a traditional leader solves day-to-day problems and helps employees do the same. ADP 6-22 (2019), strategic leadership at the military level, describes that ‘strategic leaders include military and civilian leaders at the central command […]. Strategic leadership guides and integrates multiple organizational level units that perform a wide range of functions. […] These leaders allocate resources, communicate strategic vision, and prepare their commands and the Army itself for future missions’. Strategic leadership centers on guiding complex organizations toward a lasting, shared purpose. ‘Leaders at the highest levels […] unify diverse teams with distinct roles, crafting a compelling vision that inspires commitment’ (Ligon, 2020). ‘They allocate resources strategically and equip their organizations to navigate future uncertainties’ (Samimi et al., 2022). ‘Strategic leaders nurture a culture where integrity and innovation flourish, ensuring their values motivate action across all levels’ (Ligon, 2020). ‘Drawing on experience from hands-on and mid-level roles, they refine their skills to tackle dynamic, complex challenges’ (Samimi et al., 2022). Thus, strategic leaders guide transformation efforts by planning long-term solutions which create durable progress and encourage resilience. Through the development of visionary thinking they create opportunities for others to establish impactful legacies.

Additionally, Mažeikienė (2013) argues that ‘one of the elements of ‘strategic’ is – *sustainability*. Therefore, strategic plans are developed […] years in advance. Throughout that time, leaders try to involve other people in the discussion and implementation of the plans, explaining to them the essence of the strategy and the logic behind it, inviting them to discuss it openly, and, if the situation changes, promptly improve the strategies, looking for new favourable directions, alternatives. The second key element of the term ‘strategic’ is – *the whole*. This element comprises at least two aspects. First, a strategic leader understands and sees the organization and its environment as interrelated. Not only does he or she know, but he or she also thinks ahead […] to manage the changed position […] involving as many people as possible in the organization. Second, strategic decisions have long-term implications for the whole organization, not for individual departments, teams or employees’. Moreover, Gatej (2024) notes that ‘in crisis situations there is a necessity for strategic planning, effective communication, and continuous assessment to optimize readiness and performance in crisis situations, particularly in military contexts where swift and coordinated responses are paramount for mission success and personnel safety'.

In conclusion, strategic leadership shapes the long-term direction and national security, navigating complex environments, influencing culture, and building consensus.

What are the skills and traits of a strategic leader?

Strategic leaders must profoundly understand the strategic environment, integrating military, diplomatic, economic, and psychological elements to achieve national objectives. As we delve into the skills and traits of strategic leaders, it becomes clear that their ability to inspire, adapt, and innovate is crucial for navigating the challenges of modern warfare and ensuring the success of military operations. Therefore, 'strategic leaders ideally have the ability to challenge prevailing viewpoints without provoking significant pushback, to see the big and small picture at the same time, to adapt to […] changes and take advantage of new opportunities, to make difficult decisions, to balance an analytical perspective with the human dimension of strategy building, and to advocate for and engage with employees' (Sales et al., 2023). Schoemaker et al. (2013) describe 'six critical skills that define effective strategic leadership in navigating unpredictable and high-stakes environments: *anticipate*, *challenge*, *interpret*, *decide*, *align*, and *learn*. Leaders who possess these skills can identify upcoming opportunities and dangers while challenging existing assumptions and combining intricate data to make decisions that gain stakeholder support and promote learning from achievements and setbacks'.

The President of Ukraine, Volodymyr Zelensky, exemplifies contemporary strategic leadership. All the skills and qualities of a strategic leader mentioned above are relevant to him as a person and leader. He has been able to overcome challenges and opposing viewpoints. 'Volodymyr Zelensky has become a unique example of 21st century political communication and leadership in the face of geopolitical ruptures caused by Russia's war against Ukraine. In a demonstration of moral strength and courage, the Ukrainian president refused an offer from the United States of evacuation from Kyiv' (Kriaučiūnaitė, 2023). Nevertheless, to better understand Volodymyr Zelensky's rise from a 'comedian' to a national or even global hero as a politician (leader), we need to analyze Ukraine's history and political culture in more depth and detail. There is no doubt that Ukraine's history and political culture in recent decades have created the conditions for political apathy, disillusionment and indifference, leading to two revolutions and a territorial division, bearing in mind that Ukraine only became independent in 1991. That is a very short period in geopolitics and state-building.

However, two aspects that are not necessarily essential but important are that Volodymyr Zelensky excels particularly in communication and emotional engagement. As Kriaučiūnaitė (2023) points out, 'Zelensky's political speeches have mobilized the global community to respond to Russia's invasion and to provide military, financial and humanitarian support to Ukraine. With the advent of the 21st century, emotions began to be more systematically integrated into […] international relations […]. The term *emotion* is derived from the Latin verb *motere*, meaning *movement*. […] Therefore, pertinent emotions become triggers for political mobilization of the target audience on a particular issue'.

Moreover, Kellogg School of Management (2022) highlights four principles of values-based leadership skills which makes Zelensky such a strong leader: '(1) *self-reflection* – he is thoughtful, he's self-aware, he clearly knows himself and the role he needs to play as a leader; (2) *balance* – […] he has a strong, balanced perspective of knowing he's dealing with a crisis but at the same time realizing he needs to keep that crisis in perspective so that his citizens don't lose hope; (3) *self-confidence* – he knows the role he needs to play. He's willing to be very direct with both the adversary and when talking to the […] Europe as well as […] the United States; and (4) *genuine humility* – while he's a strong personality and knows he can get a lot done, he has enough humility to realize that there's no scenario in which he's going to get through this without a lot of help from NATO and the United States'.

As Zachara-Szymańska (2023) in her article cites Keith Grint who states, 'it remains the case that individuals make a difference'. 'President Zelensky's leadership style is viewed as heroic not only because his behavior fits the description of heroism but also because he addresses the vital need of a public longing for a noble cause' (Zachara-Szymańska, 2023). Additionally, Ward (2022) cites William B. Eimicke, a professor at Columbia University's School of International and Public Affairs 'good leaders recognize that they're only as good as the people who follow them. And they are, in fact, a personification of the team of the organization […] they represent. They're not separate and apart'.

To summarise the above-mentioned and in the context of the example of the President of Ukraine, exploring the skills and traits of strategic leaders reveals that their capacity to inspire, adapt, and innovate is vital. However, the mechanism by which these qualities cascade to strengthen military organisations remains underexplored. Rather than focusing solely on Volodymyr Zelensky's broad strategic traits, such as communication or charisma, we can focus on his personal resilience – his refusal to evacuate Kyiv despite immense pressure, as noted by Kriaučiūnaitė (2023), thus reflects a capacity to withstand adversity. This resolve arguably bolstered Ukraine's military organizations by inspiring troops and unifying command structures under a shared resilient mindset. Additionally, as Kriaučiūnaitė (2023) highlighted how 'Zelensky's political speeches mobilized the global community to respond to Russia's invasion, but more critically, his steadfastness may have stabilized military morale and operational coherence, though this linkage is rarely analyzed in depth'. Similarly, the Kellogg School of Management (2022) identifies Zelensky's self-reflection and balance – traits tied to personal resilience – as key to maintaining hope amid crisis, yet how these qualities ripple into organizational resilience, such as through troop cohesion or adaptive tactics, remains a gap in scholarship. Strategic leaders, therefore, must negotiate complex settings by aligning military activities with national strategies, but their success hinges on resilience that extends beyond individual heroism. While charisma and influence, as Zachara-Szymańska (2023) notes in citing Keith Grint, 'make a difference,' the actual test lies in how personal resilience empowers organizational systems. Current literature, including Sales et al. (2023), emphasizes 'traits like challenging viewpoints and balancing analytical and human dimensions, yet it rarely explores how these foster a resilient military organization'.

Nevertheless, strategic leaders can embed such resilience into military systems through training programs that cultivate adaptive decision-making or policies that encourage learning from setbacks, fostering organizational resilience across units.

Resilience and resilient leader

Today's military faces uncertainty, complexity, and social pressures, requiring organizations to meet societal expectations while supporting soldiers. Because ‘military personnel often exhibit a higher degree of resilience compared to the general population due to the unique demands and challenges they face in their roles’ (Fernandes et al., 2024). Therefore, resilience is significant for modern armed forces and critical for organizational, unit, and individual effectiveness.

This chapter explores how individuals cultivate personal resilience through psychological techniques, particularly how resilient military leaders adapt to change while maintaining positive outlooks that motivate others during challenges.

What is resilience?

Military organizational resilience involves enduring, adapting, and recovering across three interconnected dimensions: personal strength, group dynamics, and organizational framework. Individual resilience is psychological strength that allows people to sustain their well-being even when facing stressful situations. At the group level, resilience manifests through collective cohesion and mutual support, while organizational resilience requires structural and strategic adaptability during crises. The triadic framework plays a crucial role in understanding how strategic leaders' resilience can extend to boost military resilience. For instance, ‘resilient individuals exhibit a capacity to confront adversity with a realistic outlook, derive purpose from difficult circumstances, and creatively adapt by utilizing whatever resources are accessible, as evidenced by the interplay of character strengths such as hope, bravery, and perseverance’ (Martínez-Martí et al., 2017). This personal resilience – rooted in purpose, control, and adaptability – can be a foundation for broader resilience strategies.

The Oxford Dictionary (2025) defines resilience as ‘recovering quickly from difficulties and springing back into shape’. In military contexts, psychological resilience surpasses physical preparedness, enabling adaptation to emotional and cognitive challenges.

Furthermore, Gatej (2024) notes that ‘a deeper understanding of resilience is needed not only at the individual level but also in the built environment, integrating neurobiological, cognitive, and social mechanisms that enhance adaptive functioning among military personnel during intense stressors’. Thus, it suggests that group-level resilience – fostered through shared training and support – bridges individual and organizational capacities.

From a military perspective, ADP 6-22 (2019) asserts that ‘resilience enables leaders and their organizations to endure and prevail over hardship. Resilience and commitment to accomplish the mission is critical to overcoming adversity. […] Resilient leaders learn and grow from experiencing difficult situations. Leaders instil resilience and a winning spirit in subordinates through personal example and tough, realistic training. Therefore, resilient leaders instil this quality in subordinates through example and rigorous training, thus linking personal resilience to organizational outcomes.

Strategic leaders can foster organizational resilience throughout military ranks through two complementary approaches. First – by implementing systemic mechanisms, including cascading leadership development programs, resilience-focused policies, and strategic communication frameworks that institutionalize resilience. As Bartone (2006) emphasizes ‘leaders significantly influence resilience through their attentiveness, exemplary behavior, and relationship quality with subordinates’. Second, leaders must extend personal example beyond immediate colleagues through deliberate visibility across ranks, strategic narratives, and modeling transparent vulnerability. Nordstrand et al. (2023) found that ‘military veterans display distinctive resilience profiles compared to civilian populations, highlighting the importance of leadership in developing these adaptive capacities’. This approach aligns with Kamphuis et al. (2011) research demonstrating that ‘leadership behaviors significantly influence team processes during high-stress situations’. Strategic leaders achieve optimal resilience-building through structured pathways that allow resilience modelling to flow throughout rank structures using mentoring programs, recognition systems, and communities of practice. Resilience is not just an individual quality. It is fostered by organizational structures and strengthened by leadership actions.

Moreover, Van der Meulen et al. (2020) ‘conducted a large meta-analysis of studies to provide a quantitative synthesis of longitudinal studies on the association between psychological resilience and mental health in soldiers […]. The main finding of the meta-analysis was that soldiers with higher levels of psychological resilience had fewer mental health problems. Psychological resilience was positively associated with mental health and well-being: soldiers with higher resilience have better mental health and, in the long run, rate their well-being higher’. Therefore, resilience is not an inherent moral quality but a practical skill to remain robust under significant stress, necessitating multifaceted strategies to sustain military performance. The interventions encompass personal mindfulness practices for coping enhancement, group cohesion activities for collective resilience empowerment, and organizational policies such as ongoing training to maintain structural adaptability. The concept provides a basis to explore how resilient leaders inspire broader resilience in groups and organizations while filling a significant research void in military leadership through a framework that spans individual to organizational resilience.

What are the characteristics of a resilient leader?

Military hierarchies distinguish commanders who plan tasks from soldiers who execute them, yet all require resilience training to support organizational goals. Therefore, ‘is […] a capacity that can be developed through experience, training, and deliberate practice […]’ (Robertson et al., 2015).

‘A resilient leader is a person who sees failures as temporary setbacks; they can recover from failures quickly, maintain a positive attitude, and seize opportunities during periods of turbulence. When faced with ambiguity, a resilient leader finds ways to move forward and avoids paralysis. Resilient leaders sustain their energy under pressure, adapt to disruptive changes, and prepare themselves and their teams for challenges ahead, making resilience a crucial characteristic of high-performing leaders’ (Kumar et al., 2022). Additionally, resilient leaders ‘demonstrate emotional intelligence, enabling them to regulate their emotions and empathize with their teams under stress, fostering trust and cohesion critical for team resilience' (Goleman et al., 2017). They also exhibit a 'learning orientation, viewing setbacks as opportunities for growth, continuously refining strategies to prepare for future challenges' (Dweck, 2006). Kumar et al. (2022) suggest Sir Winston Churchill as a resilience example by pointing out how he united British society throughout World War II. By demonstrating vision, courage, tenacity, and composure through his powerful speeches and visits to bombed areas, Sir Winston Churchill played a crucial role in strengthening British morale during the war. Sir Winston Churchill's leadership traits demonstrate societal resilience while providing organizational guidance on building a unified purpose and leading teams through challenging situations.

In a nutshell, leadership is about leading people; thus, the aspect of teams' cohesion is crucial and, in our case, the organization's resilience. Therefore, leader's resilience is an element of organizational and team resilience. Although the soldier is the key element in a military organization as a complex system structure, the leader must ensure the resilience of all through his/her leadership skills. Therefore, organizational and lower levels of resilience start with everyone's resilience. Nevertheless, 'while knowledge, skills, and experience provide a foundation, it is an individual's resilience that ultimately shapes their capacity to navigate challenges and achieve success' (Southwick et al., 2018).

Again, exercising Volodymyr Zelensky as an example – the world recognizes him as a capable and tenacious leader. His leadership has demonstrated tenacity and resolve despite the ongoing war. Zelensky has displayed incredible courage in handling the situation, preserving morale, and bringing the nation together. His exceptional communication skills have inspired citizens and the international community. Moreover, and to sum up, what is stated on the official website of the President of Ukraine (2024) and is mentioned by Anhelina Strashkulych and Alona Mazurenko in Ukrainska Pravda (2024) – 'in November 2024, Zelensky presented Ukraine's Internal Resilience Plan, which includes ten points aimed at strengthening the country's unity, defence capabilities, economic stability, and energy security. The plan's proposals show his proactive attitude toward creating a resilient country. Zelensky has also modified his tactics to guarantee Ukraine's survival and advancement despite the tremendous strain and difficulties. Ukraine's integration with the European Union and

NATO has advanced, and international backing has been mainly secure thanks to his leadership'.

Furthermore, synthesising the aforementioned examples of personalities and leadership characteristics supports applying the *'Servant leadership'* philosophy as a paradigmatic case, effectively illustrating the concepts discussed earlier. This philosophy was coined in 1977 by Robert K. Greenleaf. However, it remains applicable today, where he described it as a 'leadership approach that places serving others ahead of leading, a perspective that prioritizes the needs of followers over the leader's authority'. This philosophy remains relevant because it focuses on developable behaviours and practices instead of fixed traits. The philosophy supports others' development and wellness by creating an empathetic culture built on active listening, awareness, personal growth and dedication.

In conclusion, leaders demonstrate unique, essential qualities that enable them to manage complex challenges effectively. Visionary optimism allows these leaders to look past short-term challenges, and their courage and tenacity help them face significant obstacles, as figures like Churchill and Zelensky demonstrate. Additionally, emotional intelligence builds trust and empathy, strengthening team unity as learning orientation encourages constant development, enabling leaders and teams to face upcoming challenges. Self-aware and motivated leaders maintain clarity and make informed decisions under pressure, strengthening organizational resilience. Leaders who demonstrate resilience build compassionate and adaptable organizational cultures by incorporating these characteristics into their leadership approach using servant leadership principles, which focus on developing and caring for their team. Leadership qualities determine organizational resilience, demonstrating why developing these flexible traits matters for success in dynamic environments.

Resilient organization and leader's influence

'The organization's resilience is defined as a function of the organization's general awareness of the situation, the adaptability and maintaining the functioning balance in a complex, dynamic internal environment and in the system of external social and economic relations' (McManus et al., 2008). Therefore, according to Lee et al. (2013), ‘the importance of resilience becomes particularly apparent in the implementation of organizational changes, when it is important not only to introduce innovations and improve the structure but also to maintain the workflow, supply goods and services, and avoid financial losses’. Moreover, ‘anticipating future challenges is crucial in foresight because only by understanding a variety of potential scenarios can organizations prepare and adapt effectively, ensuring resilience and strategic advantage in an uncertain and rapidly changing environment’ (ACT, 2024). In this context, ‘a supportive environment for organizational change hinges on three core elements: 1) a leadership approach and organizational culture that promote adaptability to dynamic conditions, 2) internal networks that enable employees to access resources and support during change, and 3) employee preparedness for change, facilitated by clear strategic goals, structured planning, and effective communication’ (Duchek, 2020).

Furthermore, resilience in an organization includes effective management and crisis management when the organization is seeking to achieve its objectives and, simultaneously, is exposed to external factors such as uncertainty and various changes (organizational, economic, political). Additionally, Hillmann et al. (2021) describe organizational resilience as ‘the ability of an organization to integrate its internal systems and external operating environment to sustain functionality and adapt effectively amidst internal or external challenges’. Additionally, and complementing organizational resilience, Hartwig et al. (2020) ‘researched resilience at team level, discussed the concept of team resilience, examined the assumptions that strengthen this phenomenon, and the significance of teamwork processes and results’. Their research summarizes that ‘team resilience is the result of pressure, a process of effectively managing team resilience, which helps the team respond constructively to situational challenges and strengthens the team's ability to cope with future challenges. It has three main dimensions: *dynamism* (resilience is a dynamic, changing phenomenon), *adaptability* (positive adjustment to a challenging situation) and sustainable *team vitality* (endurance, the ability to sustain high performance)’.

Walker et al. (2014) state that ‘leadership has many elements. In more resilient organizations, effective leaders deal with standard and functional issues well. They plan and delegate, have effective structures, and are good at using resources’.

However, what sets effective leaders apart are their attributes and how they relate to staff and intentionally create a culture that fosters the other three factors – valuing, collaboration and learning. Resilient organizations have empowering leaders who respect their staff and earn their trust. Therefore, the military's objective of achieving overall organizational resilience is deeply linked with the personal resilience of its leaders. Effective leaders manage resources and strategies and model personal resilience traits such as ***adaptability*** and ***a positive attitude***, essential for fostering a resilient culture within the organization. This is supported by research indicating that 'leaders' personal attributes and practices play a crucial role in building cohesion and instilling purpose, thereby enhancing organizational resilience' (Coughlin, 2018). By integrating these personal resilience practices into organizational structures – through training programs, leadership development initiatives, and cultural shifts – leaders can create a cascading effect of resilience that enhances the organization's ability to adapt to dynamic environments. For instance, secure base leadership practices, which involve providing a supportive environment and modelling resilience, have been shown to enhance organizational identification and resilience through work engagement among military personnel' (Maria C. Navas-Jimenez et al., 2024). This approach emphasizes the importance of human resource management in selecting, monitoring, and maintaining resilient personnel, ensuring that psychological resilience is continuously assessed and supported. Resilient leaders are pivotal in ensuring their organizations remain adaptable and responsive to external challenges, achieving strategic advantage in uncertain environments.

Thus, to understand the impact of leadership on organizational resilience, we need to know and understand the nature of leadership itself. Leadership's theoretical significance and distinctive feature is that it requires the noncoercive and voluntary acceptance of influence. Leaders can appreciate and exert influence beyond purely positional influence, especially in the form of charisma and personal authority. Finally, a leader's actions are essential to leadership. Their influence over subordinates and understanding by subordinates are not only – *who they are* but *what they do*. There are two key aspects of effective leaders: (1) supporting the organization and its processes and (2) helping subordinates achieve organizational and personal goals.

Conclusions

Leaders must understand the ideas, procedures, and practices that shape military organisations to execute an organisational-level vision effectively. It includes navigating the relationship between influence and power, addressing the challenges of leading change, and fostering a culture and climate that promotes psychological safety and mutual trust. Leaders facilitate organisational learning while managing stress and resilience; they build cohesive teams and uphold ethical standards. Foundational elements enable organisations to adapt and maintain strong performance while remaining resilient in changing environments.

The analysis of leadership literature and military doctrine reveals that strategic leaders must inspire and provide long-term vision and establish structured pathways – such as mentoring programs, recognition systems, and communities of practice – that transmit resilience throughout all ranks. As examples like Volodymyr Zelensky and Winston Churchill demonstrate, leaders who model resilience during crises significantly impact immediate team members and the broader organizational culture. However, the specific mechanisms by which personal resilience contributes to this outcome are often implicit.

Organisational resilience grows when strategic leaders highlight strategic environment understanding and adaptability while conveying their vision. The underlying connections between personal and organisational resilience remain insufficiently understood and demand additional research. Moreover, strategic leaders' ability to draw up a strategy as a generalised plan of action over a sufficiently long period to achieve defined objectives and integrate military, diplomatic, economic, and psychological elements to achieve national objectives enhances the overall resilience of military organisations. Research findings indicate that military organisations must prioritise leadership development programs focused on strategic thinking and personal resilience for strategic leaders through training that improves adaptive decision-making and policies promoting learning from setbacks to build unit-wide resilience. Future research could explore the specific types of resilience practices most effective in different military contexts and investigate the impact of resilience-focused leadership on strategic decision-making in crises, addressing a critical gap in leadership development. Military leaders in today's complex and unpredictable world must develop personal resilience as it becomes essential for forming strong organisations that adapt to changing future challenges.

Bibliography

ADP 6-22, C1. 2019. *Army Leadership and the Profession.* Department of the Army : Washington, DC, 25 November 2019.

Allied Command Transformation. 2024. First Allied Foresight Conference. Helsinki, Finland 10-12. [Online] June 2024. https://www.act.nato.int/wp-content/uploads/2024/08/AFC_HelsinkiSummaryReport_FINAL.pdf.

Bartone, Paul T. 2006. Resilience Under Military Operational Stress: Can Leaders Influence Hardiness? *Military Psychology*, Volume 18(sup1).

Codreaunu, Aura, and Vasikescu, Cezar. 2022. [Online] *Professional military leadership development from the perspective of national resilience*. Regional Department of Defence Resources Management Studies, Brașov. DOI: 10.55535/RMT.2022.1.13. [Online] 2022. [Cited : 2025.] https://www.ssoar.info/ssoar/bitstream/handle/document/85223/ssoar-rmt-2022-1-codreanu_et_al-Professional_Military_Leadership_Development_from.pdf?sequence=1&isAllowed=y.

Coughil, Eugene. 2018. *Fostering resilience: leader strategies and practices for overcoming adv coming adversity in military organizations.* [Online, Doctoral thesis] Pepperdine University. 2018. [Cited : 2025.] https://digitalcommons.pepperdine.edu/etd/913/.

Duchek, Stephanie. 2020. Organizational resilience: a capability-based conceptualization. *Business Research*. Volume 13, pp. 215-246.

Dweck, Carol S. 2006. *The New Psychology of Success*. New York : Random House.

Fernandes, Subedar F Antony, Madhulika, Varsha. 2024. *Psychological Well-being in Military Organizations: Fostering Resilience and Performance.* Journal of the Indian Academy of Applied Psychology. Jan 2024, Vol. 50, No. 1, pp. 367-380.

Gatej, Emil Răzvan. 2024. Resilience in Military Contexts: Enhancing Performance in Crisis Situations. *Scientific Research and Education in the Air Force - AFASES 2024*. DOI: 10.19062/2247-3173.2024.25.12. [Online] 2024. [Cited : 2025.] https://www.afahc.ro/ro/afases/2024/Volume-AFASES2024/12-EmilGATEJ.pdf.

Goleman, Daniel, and Boyatzis, Richard E. 2017. Emotional Intelligence Has 12 Elements. Which Do You Need to Work On? *Harvard Business Review*. [Online] 6 February 2017. [Cited : 2025.] https://www.proveritas.com.au/downloads/Emotional-Intelligence-12-Elements.PDF.

Greenleaf, Robert K. 1977. *Servant Leadership – A Journey into the Nature of Legitimate Power and Greatness*. Paulist Press.

Guillot, W Michael (COL). 2003. Strategic Leadership. Defining the Challenge. *Air & Space Power Journal.* Winter 2003. Volume XVII, No.4. pp. 67-75. [Online] 2003. [Cited : 2025.] airuniversity.af.edu/Portals/10/ASPJ/journals/Volume-17_Issue-1-4/win03.pdf.

Halvorson, Kristina. 2025. What Is Strategy (and Why Should You Care)? *BrainTraffic.* [Online] 2025. [Cited : 2025.] https://www.braintraffic.com/blog/what-is-strategy-and-why-should-you-care.

Hannah, Sean T. 2012. *Leadership in the profession of arms*, in M. G. Rumsey (Ed.), Oxford handbook of leadership. New York, NY: Oxford University Press.

Hartwig, Angelique, Clarke, Sharon, Johnson, Sheena, and Willis, Sara. 2020. Workplace team resilience: a systematic review and conceptual development. *Organizational Psychology Review*, 10, pp. 169–200. DOI: 10.1177/2041386620919476. [Online] 2020. [Cited : 2025.] https://www.researchgate.net/publication/340844551_Workplace_team_resilience_A_systematic_review_and_conceptual_development.

Hillmann, Julia, and Guenther, Edeltraut. 2021. Organizational Resilience: A Valuable Construct for Management Research? *International Journal of Management Reviews*, Vol. 23, pp. 7–44 (2021).

KelloggInsight. 2022. What makes Zelesnky Such a Strong Leader? *The Insightful Leader*. *Kellogg School of Management* [Online] 23 MARCH 2022. [Cited : 2025.] https://insight.kellogg.northwestern.edu/newsletters/what-makes-zelensky-such-a-strong-leader.

Kriaučiūnaitė, Elžbieta. 2023. *The Zelensky Phenomenon.* Vilnius University Institute of International Relations and Political Science. [Online] 26 July 2023. https://www.tspmi.vu.lt/en/comments/the-zelensky-phenomenon/.

Kumar, A. Kishore, Kumar, K. Ajay. 2022. Resilient Leadership – Case Study of Sir Winston Churchill. *Internation Journal on Leadership*, 10 (1) 2022, pp. 36-40.

Lee Howell. 2013. Resilience: What it is and why it's needed. *Resilience: A journal of strategy and risk*, 3(2013).

Lee, Jennifer E. C., Sudom Kerry A., Zamorski Mark A. 2013. Longitudinal analysis of psychological resilience and mental health in Canadian military personnel returning from overseas deployment. *Journal of Occupational Health Psychology*, 18(4), 500. DOI: 10.1037/a0034241.

Ligon, Andrea. 2020. *The Role of Transformational Leadership in Organizational Innovation and Sustainable Success*. Murray State University. [Online, Bachelor thesis] Spring 2020. [Cited : 2025.] https://digitalcommons.murraystate.edu/bis437/261/?utm_source=digitalcommons.murraystate.edu%2Fbis437%2F261&utm_medium=PDF&utm_campaign=PDFCoverPages.

Małgorzata Zachara-Szymanska. 2023. The return of hero-leader? Volodymyr Zelensky's international image and global response to Russia's invasion of Ukraine. *Leadership*, 2023, Vol. 19(3) 196-209. DOI: 10.1177/17427150231159824.

Martínez-Martí, María Luisa, Ruch, Willibald. 2017. Character strengths predict resilience over and above positive affect, self-efficacy, optimism, social support, self-esteem, and life satisfaction. *The Journal of Positive Psychology*, 12:2, pp. 110-119.

Mažeikienė, Jolita. 2013. *Strateginė lyderystė - be rampų šviesos*. [Strategic leadership - without the spotlight]. *Verslo Žinios. Akademija.* [Online] 22 December 2013. [Cited : 2013.] https://www.vz.lt/archive/article/2013/12/22/strategine-lyderyste-be-rampu-sviesos.

McManus, Sonia, Seville, Erica, Vargo, John, & Brunsdon, David. 2008. Facilitated process for improving organizational resilience. *Natural Hazards Review, 9*(2), 81-90. doi: 10.1061/(ASCE)1527-6988(2008)9:2(81).

Merriam-Webster Dictionary. STRATEGY Definition & Meaning. *Merriam-Webster*. [Online] 2025. https://www.merriam-webster.com/dictionary/strategy#:~:text=%3A%20the%20science%20and%20art%20of%20employing%20the,support%20to%20adopted%20policies%20in%20peace%20or%20war.

van der Meulen, Erik, van der Velden, Peter G., van Aert, Robbie C. M., van Kamphuis, Wim, Gaillard, Anthony W. K. and Vogelaar, Ad L. W. 2011. The Effects of Physical Threat on Team Processes During Complex Task Performance. *Small Group Research*. Volume 42, Issue 6.

Millen, Raymond. 2012. Cultivating Strategic Thinking: The Eisenhower Model. *Parameters: The U.S. Army War College Quarterly,* Volume 42, Number 2. doi:10.55540/0031-1723.2640.

Miniotaitė, Alisa. 2022. Lyderio Dilema: Asmens, organizacijos, tautos atsparumas. Pamiršta perspektyva [The Leader's Dilemma: Resilience of the Individual, Organization, and Nation. A Forgotten Perspective]. I*nternational Coaching Community. Alisa Management Laboratory*. [Online] 28 June 2022. https://icckoucingas.lt/naujienos/lyderio-dilema-asmens-organizacijos-tautos-atsparumas-pamirsta-perspektyva/.

Mintzberg, Henry. 2024. The Mintzberg 5 P's of strategy: definition and uses. *Indeed.com.* 2024. [Online] Updated 21 November 2024. [Cited : 2025.]https://uk.indeed.com/career-advice/career-development/mintzberg-5-ps-of-strategy.

Navas-Jimenez, Maria C., *et al.* 2024. Secure Base Leadership in military training: enhancing organizational identification and resilience through work engagement. *Frontiers in Psychology*. DOI: 10.3389/fpsyg.2024.1401574.

Nazri, Mohammad, Rudi, Mohamad. 2019. Military leadership: A systematic literature review of current research. *International Journal of Business and Management*, 3(2), pp. 01-15.

Nordstrand, Andreas Espetvedt, *et al.* 2023. Differences in resilience profiles between military veterans and the general population: An exploratory latent profile analysis using the HUNT-4 survey, *Stress and Health*, Volume 40, Issue 3. [Online] June 2024. [Cited : 2025.] https://onlinelibrary.wiley.com/doi/epdf/10.1002/smi.3343.

Northouse, Peter G. 2022. *Leadership Theory and Practice.* Ninth Edition. Western Michigan University. SAGE Publications. 2022.

President of Ukraine Volodymyr Zelenskyy. 2024. Volodymyr Zelenskyy Presented Ukraine's Internal Resilience Plan. *Official website*. [Online] 19 November 2024 [Cited : 2025.] https://www.president.gov.ua/en/news/volodimir-zelenskij-predstaviv-plan-vnutrishnoyi-stijkosti-u-94505.

Robertson, Ivan. T., Cooper, Cary L., Sarkar, Mustafa, & Curran, Thomas. 2015. Resilience training in the workplace from 2003 to 2014: A systematic review*. Journal of Occupational and Organizational Psychology,* 88(3), pp. 533–562.

Sales, Francesca, Holak, Brian. 2023. What is strategic leadership? Definition. Strategic leadership. *TechTarget*. [Online] 2023. [Cited : 2025.] https://www.techtarget.com/searchcio/definition/strategic-leadership.

Samimi, Mehdi, Corte, Andres Felipe, Anderson, Marc H., Herrmann, Pol. 2022. What is strategic leadership? Developing a framework for future research. *The Leadership Quarterly*, 33(3).

Schoemaker, Paul J.H., Krupp, Steve and Howland, Samantha. 2013. Strategic Leadership: The Essential Skills. *Harward Business Review*. January-February 2013.

Singleton Sr., Jesse 2024. *Supply chain leadership in crisis: the military model for resilience.* Scientific Bulletin Vol. XXXIX, No. 1(57).

Southwick, Steven M. & Charney, Dennis S. 2018. *Resilience: The Science of Mastering Life's Greatest Challenges.* Cambridge University Press.

Strashkulych, Anhelina, and Mazurenko, Alona. 2024. Zelenskyy names 10 points of internal Resilience Plan. *Ukrainska Pravda*. [Online] 19 November 2024. [Cited : 2025.] https://www.pravda.com.ua/eng/news/2024/11/19/7485253/.

Veldhoven, Marc J. P. M. 2020. *Longitudinal associations of psychological resilience with mental health and functioning among military personnel: A meta-analysis of prospective studies.* National Library of Medicine. National Center for Biotechnology Information.

Walker, Bernard *et al*. 2014. Building Adaptive Resilience. High-performing today, agile tomorrow, thriving in the future. Ministry of Business, Innovation, and Employment, New Zealand. [Online] 2017. [Cited : 2025.] https://www.resorgs.org.nz/wp-content/uploads/2017/07/Resilient_Organisations_Building_Adaptive_Resilience_online_version.pdf.

Ward, Marguerite. 2022. Volodymyr Zelenskyy embodies resilience. It's one of multiple traits business leaders can mimic in tough times. *Business Insider Africa*. [Online] 07 April 2022. [Cited : 2025.] https://africa.businessinsider.com/strategy/volodymyr-zelenskyy-embodies-resilience-its-one-of-multiple-traits-business-leaders/sjys9cj.

Xiao, Lei, and Cao, Huan. 2017. Organizational Resilience: The Theoretical Model and Research Implication. *ITM Web of Conferences* 12, DOI: 10.1051/itmconf/20171204021.

COL Martin Novák. Will Artificial Intelligence make human strategic planning obsolete?

Introduction

AI doesn’t replace strategic thinking,
it accelerates it
(Tom Davenport)

Artificial intelligence (AI) is a groundbreaking technology of our age. Not noticed by everyone, AI is no longer science fiction; it is already a technology that influences our lives. Starting from basic applications like phone face ID, virtual agents on web portals, voice assistants, and social media applications to sophisticated military applications. Some known personalities are fearful of AI. The technology entrepreneur Musk compares the development of AI to ‘summoning the demon’ and guesses that AI is probably ‘our biggest existential threat’ (Gibs, 2014). Professor Stephen Hawking said that ‘the development of full artificial intelligence could spell the end of the human race’ (Cellan-Jones, 2014). However, not everyone refers to a dystopian future. Others believe in its great potential, claiming that ‘[AI] is going to change the world more than anything in the history of mankind. More than electricity’ (Clifford, 2019). AI brings many opportunities. AI is a key technology that enabled the fourth industrial revolution and the seventh military revolution (Reding, et al., 2023). However, AI is not only a revolution. It can potentially change the patterns of our societies in many areas (AI Action Summit, 2025). Similarly to any other new technology, AI has enormous military importance. The Russian president said in 2017 to the students, ‘whoever becomes the leader in this sphere will become the ruler of the world’ (Gigova, 2017). With all AI potential, the question arises: Will AI make human strategic planning obsolete?

Even though AI is a major technological game changer, this paper argues that AI will not make human strategic planning obsolete in the foreseeable future. AI will be a significant enabler; however, human decision-making will remain irreplaceable. To support this argument, the individual segments of the paper will describe the researched findings. The paper provides the necessary definitions of AI. Next, it describes the beginning and expectations of AI. Then, it investigates approaches to AI and lists its advantages and disadvantages. Also, it examines questions of ethics and legality. Further, it categorises military applications of AI and discusses AI's influence on strategy. Finally, the paper summarises the findings and offers recommendations for the future. The paper aims to understand better the implications of AI in military applications and its impacts on strategic planning.

Definition of AI

What is AI? There is a lack of international consensus, and definitions quickly evolve. The father of AI, John McCarthy, defined it in 1955 as ‘the science and engineering of making intelligent machines’ (Olivero, 2023). NATO Science & Technology Organisation currently uses The US Air Force definition: ‘AI refers to the ability of machines to perform tasks that normally require human intelligence – for example, recognising patterns, learning from experience, drawing conclusions, making predictions, or taking action – whether digitally or as the smart software behind autonomous physical systems’ (The DoD AI Strategy, 2019). In essence, it is a machine’s capability of learning, reasoning, problem-solving, language processing, and even perceiving (ISO, 2024).

AI can be categorised according to capabilities and functionalities. For this paper, classification based on capabilities is sufficient; three kinds of AI exist:

1. Narrow AI (ANI or weak AI) equals or exceeds human performance in a specific limited task or area. AI exists in many applications.
2. General AI (AGI or strong AI) equals full human performance at any task. AI exists as a theoretical concept only.
3. Super AI (ASI or superintelligence) exceeds human performance at any task. AI exists as a theoretical concept only (De Spiegeleire, et al., 2017 pp. 26-30).

General AI, and later Super AI, is the holy grail of AI development. It is unlikely that AI will reach this level within the next 20 years (Reding, et al., 2023). Since narrow AI is the only existing category, research will focus on this group of AIs.

Beginning and expectations of AI

Contrary to the beliefs of many, AI is not a recent scientific field. It has been with us for seven decades, starting history in 1956. Through its evolution, AI experienced periods of rapid growth with high expectations, followed by periods of decrease, also called summers and winters of AI (see figure 1) (Toosi, et al., 2022).

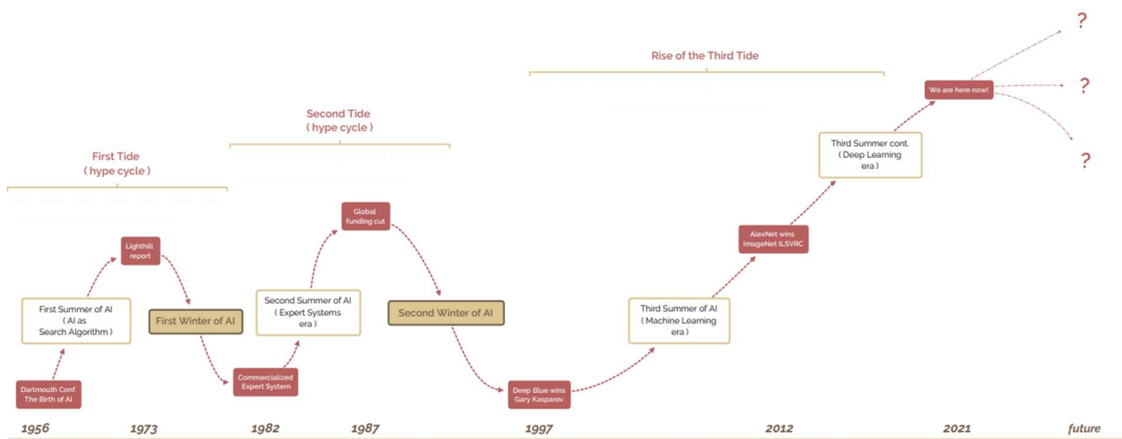

Figure 1. History of AI in three recurring cycles
Source: (Toosi, et al., 2022)

Deep learning attracted attention in 2016 when Deep Mind's AlphaGo defeated world champion Lee Sedol (Silver, et al., 2016). DARPA's AlphaDogfight Trials in 2020 is a military application example of advanced AI technology. This time, the F-16 AI agent won 5-0 against an experienced F-16 pilot in simulated dogfights (DARPA, 2020), another proof that AI can surpass human-level performance. It is necessary to remember that even though AI can outperform humans, it is still a narrow AI that is trained and excels in limited areas. The results of AlphaGo would be worse if conditions differed from the board used for training (Scharre, 2023 pp. 262-270).

Despite enormous expectations, general rules indicate that technological development is cyclic. The Gartner Hype Cycle, based on the sociology of technology adoption, can be used to describe the cycle. A hype cycle is built on the fact that technology that does not fail in the evolution process typically passes through five phases. These are:

1. Innovation Triggers.
2. Peak of Inflated Expectations.
3. Trough of Disillusionment.
4. Slope of Enlightenment.
5. Plateau of Productivity (Reding, et al., 2023).

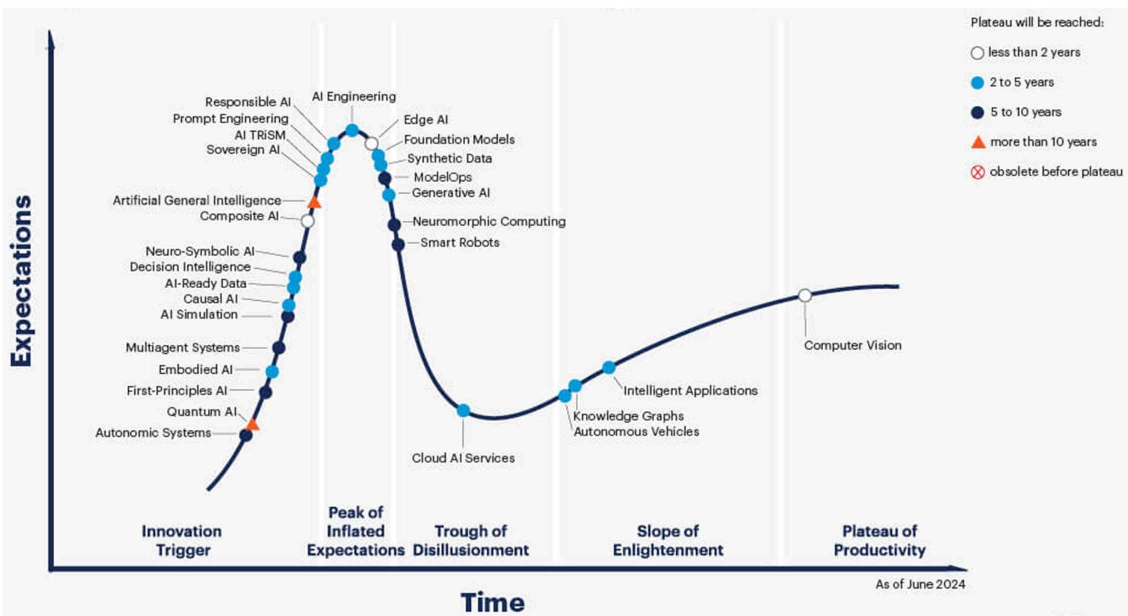

Figure 2. The Gartner Hype Cycle for Artificial Intelligence, 2024
Source: (Jaffri, 2024)

The Hype Cycle for Artificial Intelligence (see figure 2) shows that most AI applications lie within two initial phases to become mainstream innovation (Jaffri, 2024). However, some say that the Hype Cycle is not an exact science and that not all technologies follow the cycle (Gerard, 2019).

Attitudes towards military AI applications vary. Three attitudes can be identified: enthusiasts, pragmatists and deniers. Enthusiasts believe that AI will bring significant revolution into warfare. Pragmatists claim that AI will influence the war and make operations more efficient but with impact limited to tactical and operational levels.

Deniers accept the existence of AI but see limited use only in structured and controlled environments. The former indicates that only enthusiasts would support the idea that AI will significantly influence human strategic planning (Raska, et al., 2023 pp. 13-18).

Approaches to military applications of AI

Unlike other military technology, AI evolution is primarily driven by the private sector. Despite that, previously explored attitudes clearly understand AI's importance in the military domain. AI can influence the military in three fundamental roles: analytical enabler, disruptor and force multiplier. Each of these roles will be examined separately in the following paragraphs (Raska, et al., 2023 pp. 18-23).

AI as an *analytical enabler* is particularly beneficial in data-heavy areas that require fast and reliable analysis. One of those areas is Intelligence, Surveillance and Reconnaissance (ISR), where an overload of data is already present and, therefore, connected with significant investments (Morgan, et al., 2020 pp. 17-20). Connecting AI, Big Data and machine learning aims to automatically analyse hours of drone footage or pages of written reports. The US DoD's known project MAVEN used a computer vision algorithm to analyse large volumes of full-motion drone data and develop object detection or targeting that can support military and civilian analysts (Pellerin, 2017). The project also shows one of the weaknesses of AI, which is reliance on training data. When deployed to real-time environments in Iraq and Syria, the performance dropped due to the difference between training data and the actual operating environment. Used algorithms needed to be adjusted (Scharre, 2023 pp. 69-77). Apart from analytic functionality, AI can find data correlations, spot trends or changes, and map networks with potential for predictions (Horowitz, 2018). Practically, AI technology was used in 2021 during the war between Israel and Hamas for analysis and extraction of intelligence. Analytic capability enabled the identification and destruction of Hamas tunnels. The algorithm also flagged potential targets in real time and provided target suggestions for the Air Force (Ahronheim, 2021). Another practical example is the Joint All Domain Command and Control Concept developed by allies. The concept requires AI by design to fuse data from various sensors in all domains, create a single source of information and share them efficiently to fasten the decision-making process (Hoehn, 2022).

AI as a *disrupter* must be considered for our operations. AI is used to automate the creation and spread of disinformation, especially in the online domain. Russia influenced the US presidential election in 2016 using troll farms on social networks to spread disinformation (Polyakova, 2018). Natural language processing applications enforced by deep learning, e.g. ChatGPT, allow adversaries similar techniques but in text form. AI can precisely profile individuals and predict their preferences. Consequently, it is possible to identify influence-sensitive people and precisely target their fears, beliefs and weaknesses (Rosenbach, et al., 2018). Another disrupting use of AI is Deepfake, which is capable of modifying sound, video, or pictures that might erode trust in what we see and, therefore, have a malicious influence on society. Deepfake can be misused for cyberattacks, specifically phishing attacks. Satellite imagery can also be modified by the technology, which might lead to severe consequences in military planning (Vincent, 2021).

AI as a *force multiplier* refers primarily to autonomy, specifically to drones and drone swarms. Autonomy is the way to keep pace with the increasing speed of war. A certain level of autonomy built into weapons systems brings significant advantages. Autonomous systems are already used in battlefields. AI is focused on recognition and targeting. Recent AI-equipped weapons systems still rely on human operators. Three categories of interaction between weapons system autonomy and human supervision are defined:

1. Human-in-the-loop (semi-autonomous systems): The human selects a target and attacks.
2. Human-on-the-loop (human-supervised autonomous system): The system selects a target and attacks with human oversight.
3. Human-out-of-the-loop (fully autonomous system): The system selects a target and attacks without human interaction (Noone, et al., 2015).

Recently, the first two categories of automated weapons systems exist and are deployed. Predator Unmanned Aerial Vehicle is an example of a human-in-the-loop system. Israel’s Iron Dome is an example of the human-on-the-loop system. The third category, fully autonomous systems, exists limited to narrow specific tasks, such as active protection weapons on tanks or loitering ammunition designed against radars (ICRC, 2021).

Drone swarms are excellent examples of a force multiplier using AI. Swarms are not several drones flying together; they are a single communicating and cooperating system that collectively decides. Israel used technology during the combat in Gaza to locate, identify and destroy the enemy (Kallenborn, 2021). Many cheap drones formed into swarms can easily overwhelm enemy air defence by engaging the targets, reorganising for losses and spreading to avoid attack.

Benefits of AI in the military domain

Precise categorisation of benefits that AI can deliver to warfighting does not exist. RAND offers a list based on answers from the experts interviewed (see figure 3).

The first identified benefit of AI is its ability to *increase the speed* of decision-making, explicitly considering the OODA loop. With a faster processed OODA loop, adversaries are outpaced and limited in counteractions needed for defence. The second benefit is the ability to use *Big Data*, which is particularly important when the volume of collected data exceeds the human capacity to process them. As data volumes grow, the importance of ability is expected to increase. The following AI benefits are *targeting and vision*. Improved computer vision through sensors and developed targeting capability are helpful, especially with Big Data. Automated recognition surpassed human ability and can identify objects that humans would miss. Another AI benefit is *decision-making support*. Recent progress in gaming and assistance technology promises that AI can recommend options more quickly and effectively than humans. Routing technology, which is able to process maps and real-time traffic data, can be applied for logistics or scheduling. Furthermore, previous success in game applications like Go or Chess indicates potential in strategic planning. Even if unsuitable for combat decisions, it can support wargaming and red-teaming events, blunder-detection assistance, or personnel training. Next is *the mitigation of manpower* in areas where AI can replace or assist humans. An example can be image analysis or translation, but also robotic assistance in battlefield expanding warfighting capacity without increasing human resources (Morgan, et al., 2020 pp. 15-20).

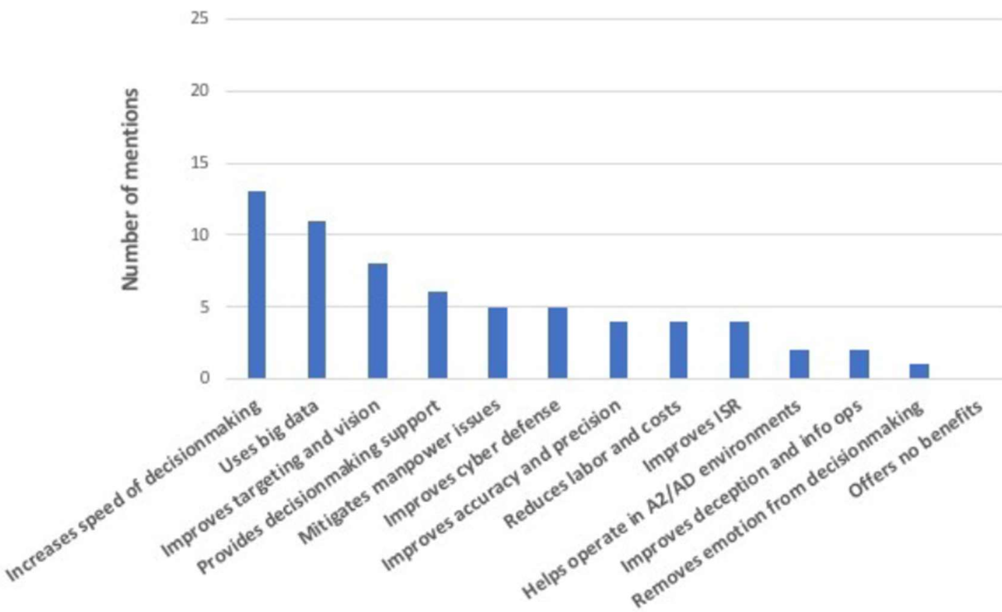

Figure 3. Potential benefits of Military applications of AI
Source: (Morgan, et al., 2020)

Cyber defence is the next AI benefit, as cyber warfare is a growing military concern. AI can enhance malware detection through data analysis of data sets and flag suspicious activity. DARPA's Cyber Grand Challenge illustrates interest in systems that can find and patch vulnerabilities or attack enemy systems. The following AI benefit is *accuracy and precision* because machines generally have better results than humans. AI is precise in situations when humans tend to think in estimates. Machines also maintain uniformity between units or over time, while people vary between individuals or experience fatigue. Another possible benefit is *labour and cost reduction* as AI or robots can take over tasks of dedicated persons, reduce personnel or entirely automate work. AI can optimise processes, which leads to cost reduction. With many complex and expensive military processes, such as logistics or recruiting, AI offers improved efficiencies and cost savings opportunities. Furthermore, the military benefits from AI capability in *Intelligence, Surveillance, and Reconnaissance (ISR)*. Combined with previous benefits, AI supports autonomous intelligence collection via drones, sensors or cyberspace and analyses vast amounts of data at high velocity. The following AI benefit is *the ability to operate in Anti-Access/Area-Denial Environments*, which is not only about risk mitigation to human operators but also about using smaller, faster and more agile weapons platforms that might be more combat capable. The last

AI benefit is *deception and information operations*. AI agents can autonomously generate content and engage in contact with a target audience to promote a particular narrative. The probability of success can be increased by tailoring content through data analysis. Another area is the use of false images, videos or audio (Morgan, et al., 2020 pp. 15-20), (Soni, 2021).

Risks of AI in the military domain

Although AI delivers major benefits, it also represents significant risks. Similarly to benefits, experts were interviewed about risks (see figure 4). The research results show that significant concerns were raised. These concerns formed three broad areas.

The first area is *the risk of error*. Experts expressed doubts about the impacts of the increased speed of AI. AI might make decisions too quickly or be unable to adapt to complex situations and, as a result, fail to distinguish combatants and noncombatants. When associated with autonomous control over nuclear weapons, failure would be catastrophic (Weissman, et al., 2024 p. 12). The second area identifies *the increased risk of war*. Conflicts could escalate due to the decreased cost of war with regard to human lives as AI systems are deployed, which could encourage commanders to act more aggressively. Another contributing factor might be the proliferation of AI-enabled autonomous systems that might lead to lower sensitivity to political considerations and next escalations. The third area expresses *the risk of the operator's overconfidence in AI capabilities*. Too high trust might lead to confirmation bias and not paying enough attention to the outputs of AI systems. Lack of understanding of AI complexity might result in unexplainable outputs (Morgan, et al., 2020 pp. 21-23). The high performance of AI systems might lead to confirmation and action bias. Israel's forces used an AI-based decision support system in Gaza for targeting. Operators' trust grew to the extent that targets were considered and approved after only 20 seconds, and they appeared to display cognitive offloading to AI (Layton, 2025).

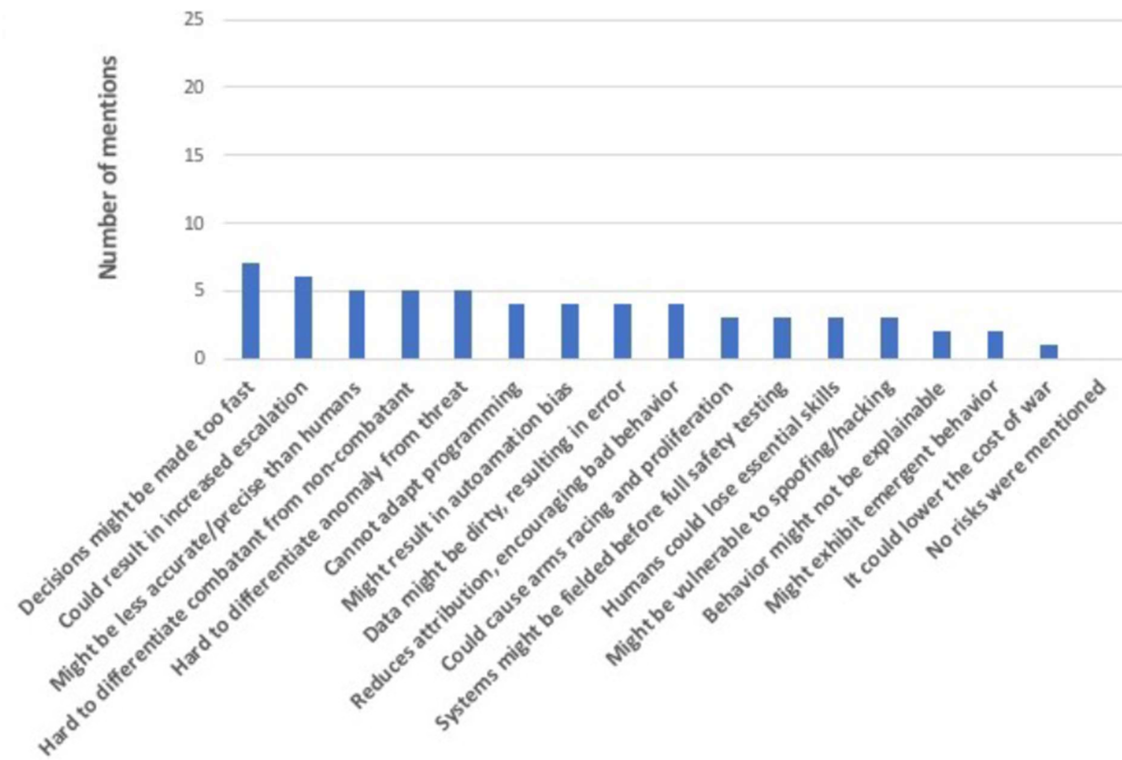

Figure 4. Potential risks of Military applications of AI
Source: (Morgan, et al., 2020)

Additionally, there is a long list of risks to be considered. Primarily, all benefits of AI become risks when used by opponents. AI agents in the cyber domain are practical examples. Technologically strong opponents can use AI to find and exploit our weaknesses in cyber defence. Using deepfakes on the battlefield constitutes a grave risk (Weissman, et al., 2024 p. 13). A team of researchers from The Hague Centre for Defence Studies identified additional risks to society and grouped them into four major categories: judicial, democratic, ethical and military (van Manen, et al., 2023 pp. 49-50). Most of them are out of the scope of this paper; however, ethical risks are generally recognised and will be explored in the next part of the paper.

Ethical and legal concerns

This section of the paper explores ethical and legal concerns related to the military application of AI. While the greatest concerns refer to Autonomous Weapons Systems (AWS), other AI military applications cannot be underestimated. When assessing ethical and legal concerns, literature mentions International Humanitarian Law (IHL), Low of Armed Conflict (LOAC), and fundamental ethical concerns for humanity.

The most feared AI application is, with no doubt, AWS. The International Committee of the Red Cross (ICRC) states that such systems, by design human-out-of-the-loop, constitute a primary ethical concern to humanity, as it is a machine that makes decisions in life-and-death situations. The unpredictability of systems can cause harm to protected persons. The systems are indiscriminate by design, which conflicts with IHL. It is hard to imagine an actual combat situation with AWS used to target humans that would not constitute a risk to IHL violations. Consequently, ICRC recommends banning unpredictable AWS, ruling out the use of AWS to target humans and designing AWS to specific targets, scope, and situations with requirements for human interaction (ICRC, 2021). The UN Secretary-General supported the unacceptability of machines taking human lives autonomously (UN, 2019). What is entirely unacceptable is autonomous control over nuclear weapons. Nuclear attack caused by AI error would have catastrophic consequences (Weissman, et al., 2024 p. 12).

Similar principles apply to also other AI applications, such as Decision Support Systems (DSS). LOAC, with its fundamental principles of proportionality, distinction and necessity, is not relevant only to AWS. Distinguishing combatants from noncombatants in congested urban areas is a challenging task, considering the principle of distinction. Also, the principle of proportionality can hardly be based on quantitative data and ethical human assessment is required (Morgan, et al., 2020 pp. 30-32). Likewise, accountability of AI systems poses another challenge. Accountability aims to deter harmful actions, responsibility for legal actions, and moral responsibility for actions. Regarding AI-supported systems, it might not be clear who is responsible. AI systems must be designed to enable accountability (Morgan, et al., 2020 pp. 32-34). Further, human dignity is the next vital moral concept. Some argue that human dignity contrasts with the concept of machines taking human lives and that only humans are capable of such a moral judgment. Others add that human emotions play an important role in just warfare as they enable warfighters to feel compassion and respect (Morgan, et al., 2020 pp. 34-35).

Additionally, human rights and privacy violations are already proven concerns. Together with sensors, AI systems' permanent surveillance supported by face recognition and analytic tools can lead to significant privacy violations (Morgan, et al., 2020 p. 35). When used by autocratic regimes, human rights are in danger. Scharre describes the AI-enabled dystopian vision of extreme violation of human rights in the case of China's repression of Uyghurs. Technology is used for constant population surveillance through numerous cameras and facial recognition scanners. Checkpoints equipped with sensors control movement, collect data and compare them with an enormous biometric database. Algorithms permanently evaluate data for potentially dangerous behaviour and enable regime control of people (Scharre, 2023 pp. 98-104).

The dual use of AI technology also raises ethical concerns as AI evolution is primarily driven by the private sector, and developments are later used in military applications. One example is Project MAVEN, which used computer vision to analyse drone footage. Pentagon cooperated with Google on evolution; however, Google employees objected to doing business of war (Raska, et al., 2023 pp. 59-76).

As a recognition of risks and risk awareness, in its 2021 AI strategy, NATO adopted six principles of effective and responsible use. Allies commit to ensure that AI guarantees:

1. Lawfulness: AI will respect all applicable laws, national, international, humanitarian, human rights and others.
2. Responsibility and Accountability: AI will adopt principles of human responsibility and accountability.
3. Explainability and Traceability: AI will be understandable and transparent thanks to the application of processes for verification, validation and assessment.
4. Reliability: AI will be certified to ensure its safety and security.
5. Governability: AI will allow for the detection of unintended consequences and the ability to deactivate the system in cases of unintended behaviour.
6. Bias Mitigation: AI will minimise bias in applications and data sets (NATO, 2021).

NATO principles align with the adopted Pentagon's AI ethical principles that demand AI to be responsible, equitable, traceable, reliable and governable (Weissman, et al., 2024 pp. 5-6). A unified approach is an effective way to mitigate known AI risks.

Recent military applications of AI

It might be misleading to look at AI military applications and consider solely AI. As AI is only one of the existing Emerging Disruptive Technologies (EDT), the effect of the others cannot be excluded. In practice, AI can be considered as a collection of variable systems, applications and methods that have their own developments (Black, et al., 2024 pp. 3-11). NATO Science & Technology Organisation suggests seeing AI through its convergence with other disruptive technologies. It is assessed that AI is and will be the most beneficial for military applications in synergy and interdependence:

1. Data – AI – Autonomy: Combinations of autonomous systems, sensors providing large volumes of data and AI processing bring military advantage.
2. Data – AI – Biotechnology: Synergy might contribute to discovering new drugs, targeted genetic modifications and other applications.
3. Data – AI – Materials: Combination enables the design of unique materials with new characteristics.
4. Energy – Materials – AI: AI, in combination with new materials and developments in energy storage, can support the reduction of fossil fuel usage in military operations (Reding, et al., 2023).

Apart from weapons systems, many other applications are supported or enabled by AI. The generally accepted grouping of AI applications does not exist, and literature uses different approaches to sort them. Clément groups AI according to tasks and related functional areas into four categories: Command and control (C2), Information management, Logistics and Training (Grand-Clément, 2023 pp. 14-15).

AI-enabled *C2 capabilities* are a real game changer in modern warfare. AI agents can identify persons and objects through visual recognition or other data, classify targets and assess possible interdependencies between targets. Consequently, they recommend options for the choice of weapons considering target type, environment and collateral damage estimate. AI can simulate and extrapolate future options and provide several courses of action regarding weapons effects, risk mitigation or optimal force position. A similar applies to contingency plans. AI can analyse real-time data and allocate sensors to a specific location or target (Grand-Clément, 2023 p. 16).

AI-enabled *information management* is a key element for other described functional areas. The first portion relates to processing and analysis of ISR data in all possible forms, e.g. video or imagery, including real-time sensor data. Processing includes cleaning, filtering, and fusing vast volumes of collected data. Current capabilities enable users to create 3-dimensional models from 2-dimensional images, geolocate objects or images, and identify or classify data. AI agents are trained to recognise patterns to identify incidents or hostile activity. Automatic analytic tools can extract required vital information and provide summaries. The second portion of the area relates to the cyber and information domain. Similar AI capabilities are used but tailored to specific domains. AI cyber agents monitor, analyse cyberspace and detect intruders via anomaly detection (Grand-Clément, 2023 pp. 17-19). AI can automatically respond to real-time threats faster than the operator and learn from patterns to improve defence (Cevians, 2024).

AI-enabled *logistics*, supply chains, and resource management also bring significant transformation and optimisation into operations. Modern military operations are dependent on complex logistics networks. AI agents can increase sustainability and operational readiness by optimising supply chains, increasing resource efficiency and predictive maintenance. AI applications deliver predictive analysis, inventory management and better resource availability. The data-driven analysis enables commanders to choose the best routes and modes of transport, thereby creating better responses to battlefield dynamics and influencing mission success (TMI Editorial Team, 2024). AI algorithms with medical databases can help with casualty care in dangerous, stressful situations when rapid decisions are necessary with basic triage (SDi, 2024). Additionally, AI capabilities already help with the automated scheduling of personnel and logistics planning (Grand-Clément, 2023 p. 19).

AI-supported *training and exercise* enable personnel to train in a safe virtual environment through realistic combat scenarios. Opponents’ performance is adaptable and offers a realistic experience. AI can be customised according to individual needs. Training scenarios range from combat skills to battlefield strategy. Warfighters can practice and improve their skills in a cost-effective environment that requires limited manpower (FlySight, 2023). Current capabilities also include options to estimate losses and scenario outcomes, track training progress and detect important learning situations. Simulations also use coordination with AI agents such as co-pilots (Grand-Clément, 2023 p. 20).

Apart from the above-mentioned areas, two important AI-powered practical applications are *AWS* and *DSS*. AWS and DSS significantly impact military decision-making time and time between target identification and engagement. According to ICRC, ‘DSS are computerised tools that are designed to aid humans in making complex decisions by presenting information that is relevant to the decision or proposing options for the decision maker to choose from in order to achieve a goal’ (ICRC, 2024). It is understood that DSS does not decide autonomously, and it is humans who make decisions; however, DSS influences decision-makers. ICRC definition says that ‘AWS select and apply force to targets without human intervention’ (ICRC, 2021). While DSS supports and might influence decision-makers, AWS human control is limited to activation or launch (Cevians, 2024). AWS and DSS raise concerns about AI's ethical and legal use in military applications.

AI and strategy

While AI has already proved its advantages at a tactical and operational level and has found its way to the battlefield, AI utilisation in strategic planning is not that far yet. However, the tactical use of AI has and will have a profound impact on the strategic level (Ayoub, et al., 2015). Tactical AI is shifting the character of war. Recent use of drones and decision support systems in Gaza and Ukraine shows that warfare tends to be positional, aiming for attrition of the enemy while focusing on quantitative measures. Layton argues that assumptions related to manoeuvre warfare cannot be explained to AI (Layton, 2025). On the other hand, Payne claims that AI can shift strategies towards the offensive, undermining the defence's strength. He also argues that AI can influence future strategies in unexpected areas, e.g., by decreasing stealth technology's importance (Payne, 2018 pp. 164-182). Considering the psychological aspect of war, tactical AI weapons decrease the psychological advantage of defenders and favour the initiative of attackers, as AI is not susceptible to human burdens (Scharre, 2023 pp. 296-310).

The use of AI on a strategic level still has significant limitations. Considering a purely technological perspective, narrow AI can outperform humans within specific microworlds, e.g. Chess or Go games or simulated F16 Dogfight. This clearly proves that, within its technical capabilities, strategy is the natural field of AI. AI can combine means and ways to reach a specific defined aim, often by using unexpected approaches (Alloui-Cros, 2022). The real world is, however, much more complex than narrow microworlds. As general AI is not available yet and is not foreseen to be developed in the near future, humans simply cannot be replaced.

AI can, however, support human decision-making on the strategic level. Human-machine teaming that combines the advantages of both humans and AI is often referred to as centaur warfighting. Within teaming, humans can play the role of necessary operators, moral agents and failsafe (Scharre, 2017). A similar analogy can be applied to strategic decision-making. It is essential to keep in mind the limitations of AI. Payne says that for strategic planners, AI's danger 'lies primarily in the gap between how the AI solves a problem framed by humans, and how those humans would solve it if they possessed the AI's speed, precision and brainpower' (Payne, 2021). If planners are aware of the gap, the danger is minimised. Strategists can delegate specific tasks to AI and focus on decision-making itself and on more complex tasks related to the problem, such as political or psychological components. AI can support humans by using its full potential in cognitive capabilities and processing power (Alloui-Cros, 2022). Strategic planners can use AI capability for modelling or risk assessment (Ayoub, et al., 2015).

The benefits of AI can be used for faster decision-making. AI can show opportunities, and humans decide. With faster proposals, humans can faster use opportunities and outpace opponents (NATO STO, 2023). The synergy of human planners and AI allows the creation of informed and more cohesive strategies based on large volumes of data and forecasts of future scenarios (TMI Editorial Team, 2024). AI cannot only assist with routine automated tasks but can also help to avoid human flaws, such as skewed risk judgement, sunk cost, or group thinking, and reduce the impact of stress or fatigue (Johnson, 2020).

What cannot be forgotten is that to use AI's full potential, militaries must adapt their organisational structures. With new technologies, processes and shifts in the character of war, changes are inevitable. Scharre claims that 'new technologies are useless without the right organisations' (Scharre, 2023 pp. 218-222). Similar applies to training and education. The full advantage and capacity of AI cannot be reached by AI-illiterate personnel. Educational activities and training must be delivered for military personnel to understand AI's opportunities and risks (Black, et al., 2024 pp. 85-141). Additionally, training is also necessary to understand the dynamics of future warfare (Thiele, 2023).

Recommendations

Several recommendations should be considered to remain competitive and to gain the strategic advantage of AI in the military domain as soon as possible:

1. Investments in research and development should be kept as a high priority as AI is a significant game changer not only in the military domain. Militaries that fail to develop and integrate AI through all command levels will face a crucial disadvantage in a possible conflict.
2. As AI implementation will trigger requirements for changes in military processes and structures, militaries should adapt with a pace to harmonise with AI implementation to allow all available AI benefits.
3. AI training and education should be developed and delivered not only to all operators but also to key leaders and senior officers to facilitate quick and efficient military transformation.
4. Close cooperation between military personnel, AI industry experts and policy and lawmakers should be maintained to deliver AI-powered tools that respect all agreed principles of effective and responsible use of AI and successful and timely adjustments of relevant laws.
5. All implemented AI products should be based on the human-in-the-loop principle and enable effective human oversight of decision-making from the tactical to the strategic level. AI should be implemented as an enhancer and not a replacer of strategic planners.

Conclusion

The purpose of this paper was to research AI, which is a major technological game changer, and answer the question of whether AI will make human strategic planning obsolete. On the path to reaching the desired answer, several areas were explored. The first part defines AI and classifies it by capabilities. Only narrow AI that cannot replace human strategic decision-making exists currently. Historical examples of AI applications with specific performance superior to humans are provided. The second part describes the future potential of AI applications using The Gartner Hype Cycle, showing current expectations of AI evolution with no foreseen breakthrough of generic AI. It also describes different attitudes to military applications of AI and indicates that only enthusiasts would agree that AI can replace humans. The third part classifies military AI applications into analytical enablers, disruptors and force multipliers and provides examples. The fourth part explores AI military applications' possible benefits and risks, including ethical and legal concerns. NATO and US approaches to address these risks are provided. It highlights the importance of keeping humans in the loop of decision-making. The fifth part describes and categorises the most significant military AI applications and their purpose. However, none of them indicates a replacement for human strategic decision-making. The final part focuses on mutual influence and interactions between AI and strategy. It explains the influence of tactical and operational AI on strategy. Also, it explains the possible use of AI on a strategic level in the form of decision support. To conclude, the provided research findings confirm the original thesis that AI will not make human strategic planning obsolete in the foreseeable future. AI is and will undoubtedly be a significant enabler; however, human decision-making will remain irreplaceable.

Abbreviations

AI – Artificial Intelligence

AGI – Artificial General Intelligence

ANI – Artificial Narrow Intelligence

ASI – Artificial Super Intelligence

AWS – Autonomous Weapons Systems

C2 – Command and control

DSS – Decision Support Systems

EDT – Emerging Disruptive Technologies

ChatGPT – Chat Generative Pre-trained Transformer

ICRC – International Committee of the Red Cross

IHL – International Humanitarian Law

ISR – Intelligence, Surveillance and Reconnaissance

LOAC – Low of Armed Conflict

Bibliography

Ahronheim, Anna. 2021. Israel's operation against Hamas was the world's first AI war. *The Jerusalem Post.* [Online] 05 27, 2021. [Cited: 03 22, 2025.] https://www.jpost.com/arab-israeli-conflict/gaza-news/guardian-of-the-walls-the-first-ai-war-669371#google_vignette.

AI Action Summit. 2025. Presentation. *AI Action Summit.* [Online] 01 17, 2025. [Cited: 03 22, 2025.] https://www.elysee.fr/en/sommet-pour-l-action-sur-l-ia/presentation.

Alloui-Cros, Baptiste. 2022. Does Artificial Intelligence Change the Nature of War? *Military Strategy Magazine, Volume 8, Issue 3.* [Online] 2022. [Cited: 03 22, 2025.] https://www.militarystrategymagazine.com/article/does-artificial-intelligence-change-the-nature-of-war/.

Ayoub, Kareem and Payne, Kenneth. 2015. Strategy in the Age of Artificial Intelligence. *Journal of Strategic Studies, Volume 39, Issue 5–6.* [Online] 11 23, 2015. [Cited: 03 22, 2025.] https://doi.org/10.1080/01402390.2015.1088838.

Black, James, et al. 2024. Strategic competition in the age of AI: Emerging risks and opportunities from military use of artificial intelligence. *RAND.* [Online] 09 06, 2024. [Cited: 03 22, 2025.] https://www.rand.org/pubs/research_reports/RRA3295-1.html.

Cellan-Jones, Rory. 2014. Stephen Hawking warns artificial intelligence could end mankind. *BBC News.* [Online] 12 02, 2014. [Cited: 03 22, 2025.] https://www.bbc.com/news/technology-30290540.

Cevians. 2024. Military Applications of AI in 2025. *Cevians.* [Online] 12 03, 2024. [Cited: 03 22, 2025.] https://www.cevians.com/military-applications-of-ai-in-2025/.

Clifford, Catherine . 2019. The ‘Oracle of A.I.’: These 4 kinds of jobs won’t be replaced by robots. *CBNC.* [Online] 01 15, 2019. [Cited: 03 22, 2025.] https://www.cnbc.com/2019/01/14/the-oracle-of-ai-these-kinds-of-jobs-will-not-be-replaced-by-robots-.html.

DARPA. 2020. AlphaDogfight Trials Foreshadow Future of Human-Machine Symbiosis. *DARPA.* [Online] 08 26, 2020. [Cited: 03 22, 2025.] https://www.darpa.mil/news/2020/alphadogfight-trial.

De Spiegeleire, Stephan, Maas, Matthijs and Sweijs, Tim. 2017. ARTIFICIAL INTELLIGENCE AND THE FUTURE OF DEFENSE: STRATEGIC IMPLICATIONS

FOR SMALL- AND MEDIUM-SIZED FORCE PROVIDERS,. *The Hague Centre for Strategic Studies.* [Online] 2017. [Cited: 03 22, 2025.] http://www.jstor.org/stable/resrep12564.1.

FlySight. 2023. Artificial Intelligence in Military Technology – 8 Applications & Examples. *FlySight.* [Online] 06 14, 2023. [Cited: 03 22, 2025.] https://www.flysight.it/artificial-intelligence-in-military-technology-8-applications-examples/.

Gerard, David. 2019. The Gartner Hype Cycle is … hype. Don't use it as an excuse. *David Gerard.* [Online] 10 03, 2019. [Cited: 03 22, 2025.] https://davidgerard.co.uk/blockchain/2019/10/03/the-gartner-hype-cycle-is-hype-dont-use-it-as-an-excuse/.

Gibs, Samuel. 2014. Elon Musk: artificial intelligence is our biggest existential threat. *Guardian.* [Online] 10 27, 2014. [Cited: 03 22, 2025.] https://www.theguardian.com/technology/2014/oct/27/elon-musk-artificial-intelligence-ai-biggest-existential-threat.

Gigova, Radina. 2017. Who Vladimir Putin thinks will rule the world. *CNN World.* [Online] 09 02, 2017. [Cited: 03 22, 2025.] https://edition.cnn.com/2017/09/01/world/putin-artificial-intelligence-will-rule-world/index.html.

Grand-Clément, Sarah. 2023. Artificial Intelligence Beyond Weapons: Application and Impact of AI in the Military Domain. *UNIDIR.* [Online] 10 11, 2023. [Cited: 03 22, 2025.] https://unidir.org/publication/artificial-intelligence-beyond-weapons-application-and-impact-of-ai-in-the-military-domain/.

Hoehn, John R. 2022. Advanced Battle Management System (ABMS). *US Library of Congres. Congressional Research Service, Ver. 4.* [Online] 02 15, 2022. [Cited: 03 22, 2025.] https://sgp.fas.org/crs/weapons/IF11866.pdf. IF11866.

Horowitz, Michael C. 2018. Artificial Intelligence, International Competition, and the Balance of Power. *Texas National Security Review: Volume 1, Issue 3.* [Online] 05 2018. [Cited: 03 22, 2025.] http://hdl.handle.net/2152/65638. ISSN 2576-1153.

ICRC. 2024. Decisions, Decisions, Decisions: computation and Artificial Intelligence in military decision-making. *International Committee of the Red Cross.* [Online] 04 2024.

[Cited: 03 22, 2025.] https://shop.icrc.org/decisions-decisions-decisions-computation-and-artificial-intelligence-in-military-decision-making-pdf-en.html.

—. 2021. ICRC position on autonomous weapon systems. *International Committee of the Red Cross.* [Online] 05 12, 2021. [Cited: 03 22, 2025.] https://www.icrc.org/en/document/icrc-position-autonomous-weapon-systems.

ISO. 2024. What is artificial intelligence (AI)? *ISO.* [Online] 2024. [Cited: 03 22, 2025.] https://www.iso.org/artificial-intelligence/what-is-ai.

Jaffri, Afraz. 2024. Explore Beyond GenAI on the 2024 Hype Cycle for Artificial Intelligence. *Gartner.* [Online] 11 11, 2024. [Cited: 03 22, 2025.] https://www.gartner.com/en/articles/hype-cycle-for-artificial-intelligence.

Johnson, James. 2020. Delegating strategic decision-making to machines: Dr. Strangelove Redux? *Journal of Strategic Studies, Volume 45, Issue 3.* [Online] 04 30, 2020. [Cited: 03 22, 2025.] https://doi.org/10.1080/01402390.2020.1759038.

Kallenborn, Zachary. 2021. Israel's Drone Swarm Over Gaza Should Worry Everyone. *Defence One.* [Online] 07 07, 2021. [Cited: 03 22, 2025.] https://www.defenseone.com/ideas/2021/07/israels-drone-swarm-over-gaza-should-worry-everyone/183156/.

Layton, Peter. 2025. Human-Machine Teaming's Shared Cognition Changes How War is Made. *RUSI.* [Online] 01 27, 2025. [Cited: 03 22, 2025.] https://rusi.org/explore-our-research/publications/commentary/human-machine-teamings-shared-cognition-changes-how-war-made.

Morgan, Forrest E., et al. 2020. Military Applications of Artificial Intelligence: Ethical Concerns in an Uncertain World. *RAND.* [Online] 04 28, 2020. [Cited: 03 22, 2025.] https://www.rand.org/pubs/research_reports/RR3139-1.html.

NATO STO. 2023. Using artificial intelligence to enhance military decision-making. [Online] 2023. [Cited: 03 22, 2025.] https://www.youtube.com/watch?v=A2ZAHrT3UwM.

NATO. 2021. Summary of the NATO Artificial Intelligence Strategy. *North Atlantic Treaty Organisation.* [Online] 10 22, 2021. [Cited: 03 22, 2025.] https://www.nato.int/cps/en/natohq/official_texts_187617.htm.

Noone, Gregory P. and Noone, Diana C. 2015. The Debate Over Autonomous Weapons Systems. *Case Western Reserve Journal of International Law, Volume 47,* *Issue 1.* [Online] 2015. [Cited: 03 22, 2025.] https://scholarlycommons.law.case.edu/jil/vol47/iss1/6/.

Olivero, Amy. 2023. International Definitions of Artificial Intelligence. *IAPP.* [Online] 09 2023. [Cited: 03 22, 2025.] https://iapp.org/media/pdf/resource_center/international_definitions_of_ai.pdf.

Payne, Kenneth. 2021. *I, Warbot: The Dawn of Artificially Intelligent Conflict.* London : C. Hurst and Company, 2021. ISBN 9781787384620.

—. 2018. *Strategy, Evolution, and War: From Apes to Artificial Intelligence.* Washington, DC : Georgetown University Press, 2018. ISBN 9781626165793.

Pellerin, Cheryl. 2017. Project Maven Industry Day Pursues Artificial Intelligence for DoD Challenges. *DoD News.* [Online] 10 27, 2017. [Cited: 03 22, 2025.] https://www.defense.gov/News/News-Stories/Article/Article/1356172/project-maven-industry-day-pursues-artificial-intelligence-for-dod-challenges/.

Polyakova, Alina. 2018. Weapons of the weak: Russia and AI-driven asymmetric warfare. *Brookings.* [Online] 11 15, 2018. [Cited: 03 22, 2025.] https://www.brookings.edu/articles/weapons-of-the-weak-russia-and-ai-driven-asymmetric-warfare/.

Raska, Michael and Bitzinge, Richard A. 2023. *The AI Wave in Defence Innovation: Assessing Military Artificial Intelligence Strategies, Capabilities, and Trajectories.* New York : Routledge, 2023. ISBN 9781032110752.

Reding, Dale F., et al. 2023. Science & Technology Trends 2023-2043, Volume 1: Overview. *NATO Science & Technology Organization.* [Online] 03 2023. [Cited: 03 22, 2025.] https://www.nato.int/nato_static_fl2014/assets/pdf/2023/3/pdf/stt23-vol1.pdf.

Reding, Dale F., et al. 2023. Science & Technology Trends 2023-2043, Volume 2: Analysis. *NATO Science & Technology Organization.* [Online] 03 2023. [Cited: 03 22, 2025.] https://www.nato.int/nato_static_fl2014/assets/pdf/2023/3/pdf/stt23-vol2.pdf.

Rosenbach, Eric and Mansted, Katherine. 2018. Can Democracy Survive in the Information Age? *Belfer Center for Science and International Affairs, Harvard Kennedy School.* [Online] 10 2018. [Cited: 03 22, 2025.] https://www.belfercenter.org/publication/can-democracy-survive-information-age.

Scharre, Paul. 2017. Centaur Warfighting: The false chioce of humans vs. automation. *Temple University.* [Online] 2017. [Cited: 03 22, 2025.] https://sites.temple.edu/ticlj/files/2017/02/30.1.Scharre-TICLJ.pdf.

—. 2023. *Four Battlegrounds: Power in the Age of Artificial Intelligence.* London : W. W. Norton & Company Ltd, 2023. ISBN 978-0-393-86687-2.

SDi. 2024. The Most Useful Military Applications of AI in 2024 and Beyond. *SDi Sentient.* [Online] 2024. [Cited: 03 22, 2025.] https://sdi.ai/blog/the-most-useful-military-applications-of-ai/.

Silver, David, Huang, Aja and Maddison, Chris J. 2016. Mastering the game of Go with deep neural networks and tree search. *Nature.* [Online] 01 27, 2016. [Cited: 03 22, 2025.] https://www.nature.com/articles/nature16961.

Soni, Pragya. 2021. AI in Military Sector - Advantages and Disadvantages. *Analytics.* [Online] 11 05, 2021. [Cited: 03 22, 2025.] https://www.analyticssteps.com/blogs/ai-military-sector-advantages-and-disadvantages.

The DoD AI Strategy. 2019. The United States Air Force Artificial Intelligence Annex. *The Department of Defense Artificial Intelligence Strategy.* [Online] 2019. [Cited: 03 22, 2025.] https://www.af.mil/Portals/1/documents/5/USAF-AI-Annex-to-DoD-AI-Strategy.pdf.

Thiele, Ralph D. 2023. The Impact of Evolving Technologies, Operational Concepts and Military Culture on Future Air War. *ISPSW Strategy Series: Focus on Defense and International Security, Issue 943.* [Online] 05 2023. [Cited: 03 22, 2025.] https://www.ispsw.com/wp-content/uploads/2023/05/934_Thiele.pdf.

TMI Editorial Team. 2024. The Impact of AI on Military Tactics and Strategic Operations. *Total Military Insight.* [Online] 07 17, 2024. [Cited: 03 22, 2025.] https://totalmilitaryinsight.com/impact-of-ai-on-military-tactics/.

Toosi, Amirhosein, et al. 2022. A Brief History of AI: How to Prevent Another Winter (A Critical Review). *PET Clinics, Volume 16, Issue 4, P449-469.* [Online] 12 12, 2022. [Cited: 03 22, 2025.] https://arxiv.org/pdf/2109.01517.

UN. 2019. Machines Capable of Taking Lives without Human Involvement Are Unacceptable, Secretary-General Tells Experts on Autonomous Weapons Systems. *United Nations Press Release.* [Online] 03 25, 2019. [Cited: 03 22, 2025.] https://press.un.org/en/2019/sgsm19512.doc.htm.

van Manen, Hugo, et al. 2023. Emerging Disruptive Technologies in an Era of Great Power Competition. *The Hague Centre for Strategic Studies.* [Online] 01 16, 2023. [Cited: 03 22, 2025.] https://hcss.nl/report/emerging-disruptive-technologies-in-an-era-of-great-power-competition/.

Vincent, James. 2021. Deepfake satellite imagery poses a not-so-distant threat, warn geographers. *The Verge.* [Online] 04 27, 2021. [Cited: 03 22, 2025.] https://www.theverge.com/2021/4/27/22403741/deepfake-geography-satellite-imagery-ai-generated-fakes-threat.

Weissman, Robert and Wooten, Savannah. 2024. A.I. Joe: The Dangers of Artificial Intelligence and the Military. *PublicCitizen.* [Online] 02 29, 2024. [Cited: 03 22, 2025.] https://www.citizen.org/article/ai-joe-report/.

LTC Kevin M. Ryan. More Bang for their Buck: Sustaining the Baltic Defence Strategies

LTC Kevin M. Ryan *held the position of* ***US Army War College Fellow*** *for years 2024-2025 in the Baltic Defence College, and thus participated fully in the HCSC. The views expressed are those of the author and do not necessarily reflect the official policy or position of the Department of the Army, Department of Defense, or the U.S. Government.*

> "Our overall security and defence depend on how much we spend and how we spend it. Increased investments should be directed towards meeting our capability priorities, and Allies also need to display the political will to provide required capabilities and deploy forces when needed." (NATO, 2014)
>
> -- NATO Wales Summit Declaration, 2014

The fourteenth paragraph of the 2014 North Atlantic Treaty Organisation (NATO) Wales Summit Declaration is the most consequential point made in a Summit Declaration in NATO's 75-year history. This paragraph, written just five months after Russia's illegal annexation of Crimea, committed all member nations to spend 2% of their national Gross Domestic Product (GDP) on defence expenditures and to commit 20% of that spending to the purchase of major equipment and related research and development (R&D) (NATO, 2014). At the time, only four of the twenty-eight member nations achieved these goals; the rest were given a decade to make 2 and 20% or more their aim. After eleven years, three years from a full-scale Russian invasion of Ukraine, and the addition of four new member nations, 23 of 32 members meet or exceed the 2 and 20% defence expenditure goals. The European allies and Canada have increased their collective investment from 1.43% of GDP in 2014 to 2.02% today (NATO, 2024a).

This paper will analyse the sustainability of the defence spending strategies of three of the most vulnerable nations on NATO's northeastern flank: Estonia, Latvia, and Lithuania, collectively referred to as the "Baltic nations" for their proximity to the Baltic Sea and shared national histories of oppression and freedom from Soviet occupation.

It will do so by explaining the efficacy of a defence spending strategy pegged to GDP, describing each nation's strategies, and suggesting opportunities to enhance the long-term sustainability of these strategies against a persistent and indefinite threat from Russia and its proxies.

The Cost of Credibility: NATO's Spending Targets in a New Security Era

"To Prevent War, NATO Must Spend More"

-Secretary General of NATO Mark Rutte (NATO 2024b)

Spending as Strategy: The New NATO Consensus. Expert analysis from defence economist and former advisor to the NATO Military Committee, Colonel Jordan Becker, PhD, suggests a strong causal link between spending and readiness. He writes that "investing more in defence - and in equipment, specifically - results in increased capabilities, which results in bearing an increased share of NATO's burden in terms of actual operations. It is especially noteworthy that past equipment expenditures strongly predict present deployability and sustainability, two of NATO's most critical output metrics" (Becker, 2017). Colonel Becker's analysis and the lack of a helpful alternative to assess Allied commitment to NATO suggest that spending targets must continue to be used. Since the Russian invasion of Ukraine in 2022, most NATO member states acknowledge that the 2% goal is not enough.

US President Donald Trump has declared his desire for European countries to aim at 5% for defence spending, (Posaner, Joshua; Laura Kayali, Julius Brinkmann; Oliver Noyan 2025) This is seen as an effort to reduce the US share of European security and match Russia's estimated defence budget of 6% or more. In his first speech as NATO Secretary General, Mark Rutte suggested a 4% threshold, arguing that the only way to go below 4% is by "buying better, (making) the most innovative technologies part of your defence industrial base, or by buying together" (NATO, 2024b). Unsurprisingly, the forthcoming NATO Summit at The Hague in the summer of 2025 is expected to increase the percentage of GDP spending targets for all member nations.

The Baltic Commitment: Ambition Meets Reality. To their credit, the Baltic nations have been spending over the 2% threshold for several years and have all committed to spending more in the coming years. Lithuania's Defence Minister Laurynas

Kasčiūnas agrees with Mr. Rutte on a 4% threshold (BNS, 2024). Estonian Defence Minister Hanno Pevkur suggested that the new NATO defence plans in the Baltic would increase Estonia's defence spending to over 5% of GDP (Kiisler, 2024) and Latvia's Defence Minister Andris Sprūds confirmed that "Latvia's government is united in the decision to increase defence funding to 4% of GDP (in 2025) and continue moving toward 5%" (MoD Military Public Affairs Department, 2025).

However, these small nations will struggle to sustain these commitments long-term for various reasons, as illustrated below. The Baltic would be wise to heed Mr Rutte's advice on " buying better" to decrease the stress on their economies and political will to sustain this commitment for the foreseeable future.

Small States, Strategic Stakes: The Baltic Nations' Defence Dilemma

Each Baltic nation unequivocally declares in their respective national security strategies that Russia poses the greatest threat to their national interest. This is due to their status as former Soviet republics, Russia's stated goals to return NATO to pre-1997 borders, and a larger combat-seasoned Russian armed force capable of quickly repositioning from the Ukrainian front to the Baltic border. Their geography, demographics, and economic capacity are also factors that contribute significantly to the crafting of their respective strategies.

Economic Realities and Defence Spending. The Baltic nations occupy a region the same size as the US states known collectively as "New England" (Maine, New Hampshire, Vermont, Massachusetts, Rhode Island, and Connecticut). Yet, the Baltic region has less than half the population of New England, and New England boasts an economy eight times the size of the Baltic nations' combined GDP. In real money, the combined GDP of the Baltic nations in 2025 are approximately €154 billion (~$165 billion), dramatically affecting their purchasing power in the defence realm. For a comparison, see the chart below.

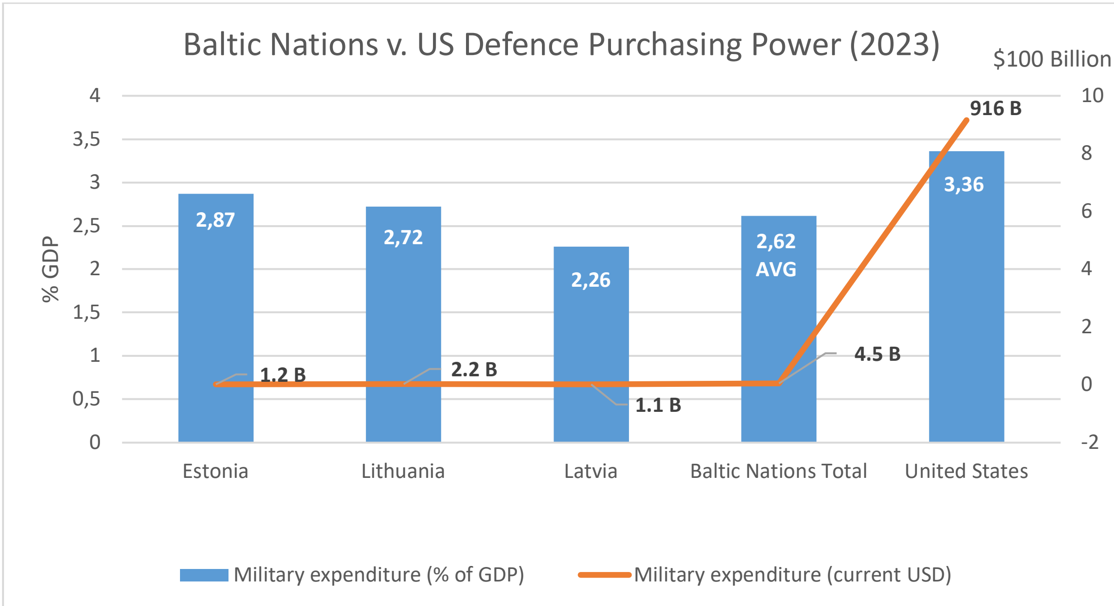

Chart 1: Baltic Nations vs. US Defence Purchasing Power (World Bank Data, 2023).

Each of the Baltic nations has its unique geography, culture, language, history, and demography that influence their national defence strategies, and while they exercise an admirable amount of defence and security cooperation, each nation, following NATO Article 3 commitment to “resist an armed attack,” must do so of its own accord. These factors have resulted in some critical differences in the national defence strategies of each country and have affected how each country spends money on defence.

Country-Specific Strategies. Estonia has the smallest hostile land border of the Baltic nations. “It enjoys terrain features like the Narva River and Lakes Peipus and Pihkva that restrict overland movement on its eastern flank and reduce its most vulnerable terrain to approximately 210km (~130 miles)” (Ryan, 2024). The northern border city of Narva has a majority ethnic Russian population. It is the closest Baltic city to one of the most strategically significant Russian cities, St. Petersburg, only 150km (~93 miles) away.

These factors have influenced Estonia’s approach to defence spending since the Russian invasion of Ukraine in 2022. The Estonians will continue investing in munitions, including small-calibre, anti-tank, short-range anti-aircraft and artillery ammunition, loitering munitions, and anti-ship missile systems (Kaitseministeerium, 2024a). The Estonian Ministry of Defence (MoD) plans to upgrade its Army's ground-based fighting platforms by purchasing 4×4 armoured vehicles, converting its CV90 combat vehicles (Kaitseministeerium, 2024a). The MoD has already procured K9 self-propelled howitzers and begun the process to upgrade their communications equipment and fight-at-night capabilities (Kaitseministeerium, 2024a). Multiple military infrastructure projects are also being worked on with a mixture of funding from NATO, the EU, and the state (Kaitseministeerium, 2024a).

Latvia, compared to Estonia, "shares a 387km (~240 miles) border with Russia and Belarus, with multiple rail and surface roads facilitating cross-border manoeuvre and virtually no terrain features impeding overland movement" (Ryan, 2024). Latvia plans to increase its defence budget to 3.45% of GDP in 2025. It will continue to grow its defence spending vis-à-vis GDP for the next three years before reducing the percentage and expenditures back down to the country's target percentage of around 3% (Ministry of Defence Latvia, 2025).

Latvia plans to spend 42% of its defence budget on procuring capabilities. This year, the country will spend over € 200 million on layer-based air defence capabilities, nearly € 140 million on ammunition and equipment, close to € 112 million on Infantry fighting vehicles, almost € 53 million on indirect fire systems, € 20 million on autonomous systems and munitions, and € 17.35 million on maritime control and coastal defence capabilities (Ministry of Defence Latvia 2025).

Lithuania and Latvia share similarities but Lithuania has nearly "nearly two and half times the border area to cover, more rail and surface roads crossing its hostile borders, and a capital just 40km from Russia's ally, Belarus," (Ryan, 2024) (Milevski, 2024) and the Russian exclave of Kaliningrad, which poses a significant anti-access and aerial denial threat. In January 2025, Lithuanian President Gitanas Nausėda and Defence Minister Dovilė Šakalienė announced that the country would spend an annual average of 5.5% of GDP on defence between 2026 and 2030, but this percentage of GDP must be approved annually by the Lithuanian Parliament (BNS, 2025). This added political pressure may make it challenging to depend on this level of spending for military procurement projects.

Regional Cooperation and the Baltic Defence Line. This increase in defence spending is intended to achieve the full operational readiness status of the new Lithuanian Division by 2030. According to the Defence Minister, this new spending agreement includes an advanced payment to acquire the German Leopard tanks required for the Division on a more accelerated timeline to ensure their delivery by 2030 (BNS, 2025). To do this, the Lithuanian government increased their borrowing limit by € 800 million, and the President committed to "certainly not go down this road where more funding for national defence is linked to a higher tax burden on the population" (BNS, 2025).

The nations also collaborate on defence initiatives, but in recent years, joint exercises between the three nations have dramatically decreased. The most enduring collaboration is the Baltic Defence College in Tartu, Estonia. This NATO-accredited professional military education institution celebrated its 25th anniversary in 2024 and has educated thousands of senior military and civilian students for NATO and partner forces. The three nations cooperate to fund this college from their collective defence budgets, contributing to the cooperation and interoperability between the Baltic nations and their allies.

The nations also recently committed to the so-called "Baltic Defence Line" (BDL), a project to connect the physical defensive barriers on the region's eastern flank. "Announced jointly by the three nations' Ministers of Defence on January 19th, 2024, the BDL is intended to connect 'anti-mobility installations' along the eastern flank of the region to deter Russian aggression and produce a capability to defend the territory from the first meter" (Ministry of Defence, 2024) (Ryan, 2024). However, this project is regionally aligned in name only, as each country embarks on its unique plan to strengthen its terrestrial defensive posture, with no clear indication that this line would connect physically or logically between countries. Moreover, the burden-sharing seems disproportionate as Latvia and Estonia have committed 8% of their total defence budgets toward the project, while Lithuania, with a larger economy, has committed just 2.8% (NATO, 2024c).

Fiscal, Political, and Demographic Constraints on Sustainability. The Baltic nations also belong to the European Union (EU), which has guidelines for member nations' deficits not to exceed 3% of GDP. The Baltic nations are fiscally responsible, with Lithuania running one of the leanest deficits in the EU and Latvia and Estonia averaging at or around the 3% threshold. However, as noted in Estonia, recent defence spending has increased the deficit to 4.4% in the coming year, causing the government to institute a 2% tax increase and austerity measures to cut € 1.3 billion from the public sector (ERR, 2024).

While tax increases and austerity will help Baltic nations keep their deficit under the EU threshold, these measures are politically unsustainable in the long term. It may also discourage significant and sustained investments in necessary projects for these nations to fund their defence initiatives effectively. If the Baltic nations are to double their nations' defence expenditures in the coming years, then they must assess the long-term feasibility of these plans so as not to exhaust the political capital they currently have on this subject.

Demographic pressures associated with an ageing population, low birth rate, low immigration, and increased emigration represent a significant long-term issue to sustaining Baltic nation defence strategies. This means the Baltic nations will have a smaller working-age population to pay for long-term military projects and fewer people to serve in military formations. Each of the Baltic nations has taken short-term measures to address demographic concerns, such as the framework nations of UK and Canada rotating forces in Estonia and Latvia respectively, and in Lithuania, the historic permanent stationing of the German 45th Panzer Brigade. While these measures bolster the low numbers in the host nation force and provide a so-called "NATO tripwire" for larger coalition force involvement in a conflict in the Baltic region, they add enormous costs via host nation support services and add very little to tax revenue.

Strategy, Society, and the Strain of Sustained Deterrence

From Punishment to Denial: A Strategic Shift. The aim of the Baltic defence strategies, like most defence strategies in Europe, is to deter Russian aggression against the states. While this paper will not address the efficacy of deterrence as a strategy, it must define what type of deterrence the Baltic are trying to achieve.

“Deterrence is the practice of discouraging or restraining a nation-state from taking unwanted actions, such as an armed attack” (Mazarr, 2018). Classical definitions delineate deterrence methods into two categories: denial and punishment. Deterrence by denial involves a demonstration of capability so strong that it convinces a potential aggressor that it would fail to achieve its objectives if attempted (Mazarr, 2018). In contrast, deterrence by punishment makes the penalty for an act of aggression so severe that it discourages an adversary from trying it in the first place (Mazarr, 2018) .

Europe’s primarily reliance on deterrence by punishment in the form of the US and UK extended nuclear deterrent through the NATO Article 5 commitment for most of its 75-year history. But Russia’s war of aggression on Ukraine and its ability to withstand crushing economic and conventional military punishment in the ensuing three years, and perceptions of uncertain US commitment, have caused these nations to embrace a strategy of denial.

The Baltic Defence Line: A Regional Denial Strategy. In the Baltic, the most visible denial strategy to date is the announcement of the Baltic Defence Line. The Baltic nations must secure the 1,360km (~845 miles) hostile border with Russia and Belarus to achieve their denial strategy. Each country has committed “an estimated € 60 million annually to the project (LRT News, 2024). Estonia intends to acquire public and private land to build approximately 600 bunkers to cover ground not otherwise restricted by natural features (ERR News, 2024). Latvia also plans to acquire land and is building up the fortification of major ground lines of communication in border regions with large ethnic-Russian populations (CSB Official Statistics of Latvia, 2024). Lithuania’s denial plan is to pre-position engineer assets that can be quickly deployed to the border region in the event of a suspected armed attack. (Česėkaitė, 2024).

While these plans are just over a year old, the classified portions of which are unavailable to the public, they are costly and require significant manpower for the Baltic nations to employ effectively. Estonia does not seem to have the active-duty manpower to effectively occupy and provide overwatch for all six hundred bunkers along its border, potentially leaving large holes in its defence line. Assets required to move the counter-mobility obstacles into place in Lithuania will be large signatures to the adversary, who could target these assets and disrupt the emplacement of critical denial architecture. Latvia may have issues acquiring the land needed in ethnic-Russian regions critical to its portion of the denial front. Russia will exploit any gap or seam in the Baltic Defence Line to establish a foothold in the Baltic, which must be accounted for in this denial plan. Furthermore, nations must regularly exercise cross-border coordination with active and reserve forces to pass targets off between national assets to reduce the possibility of an exploitable gap between nations.

Sustaining Deterrence: Political Will and Public Support. Defence strategies for the Baltic must address the threat and account for a nation's ability to sustain this commitment to national security indefinitely, especially regarding a revanchist Russia that will continue to be the region's long-term existential threat. The political will to do so in these democratic societies is linked to the population's support for these strategies and their impact on an individual's peacetime well-being.

Perceptions of Security: Patriotism, Trust, Alliances, and Investment. According to the most recent data from 2024, Estonians aged 20-39 were the least likely demographic in Estonia to take up arms in defence of their Nation if attacked, with less than half of respondents answering in the affirmative (Kaitseministeerium, 2024b). This is due to several factors related to the young and working-age population, who would rather continue to prosper in the careers they are establishing. This may also reflect the broader demographic challenges these societies face. This is the case in Ukraine, where the minimum conscription age is 25 in part to avoid a catastrophic population decline in the post-war period, which results in an average age of over 40 for Ukrainian service members (Strashkulych, 2024).

Estonians have consistently ranked their membership in NATO as their top security guarantor, ahead of armed allies stationed in Estonia and the Estonians' willingness to defend their country (Kaitseministeerium, 2024b). However, the survey data, which is current as of a year ago, had not accounted for the rapid change in popular European perception of the US commitment to the transatlantic alliance. Some of the least popular security guarantees on the list have taken centre stage in the public discourse. Estonians rank partnerships with other Baltic Nations, partnerships with Nordic countries, and investments in defence as some of the lowest guarantees of security surveyed, at 22%, 21%, and 8%, respectively (Kaitseministeerium, 2024b). It is this last statistic that is most concerning. If the Baltic Nations were to spend more, their citizens would be convinced that it would contribute significantly to their collective defence.

Sustaining Deterrence: Financing and Future-Proofing Baltic Defence

Political Will and the Limits of Public Support. At the March 2025 Annual Conference on Russia hosted by the Baltic Defence College, the Estonian Minister of Defence, Hanno Pevkur, delivered a keynote address where he expressed the country's urgent need to spend more than 5% of GDP on defence starting in 2025. When asked by the author of this paper how the nation planned to sustain such a substantial financial commitment to defence, the minister admitted that maintaining such a commitment is up to the will of the voters expressed through their representatives in parliament annually. This will require a concerted effort by politicians to raise the public consciousness on this issue and connect it effectively to perceptions of security in the Baltic region.

However, raising public support for increased spending is insufficient to ensure sustained investment in defence at the rate the Baltic nations suggest, particularly if it impacts citizens' wallets. There needs to be assistance from external entities for financial support to defer the cost for the voting population. For this, increased funding for the Baltic from NATO's Security Investment Programme (NSIP) and EU regulatory reform regarding member nation deficits and debt can help.

NATO NSIP: Investing in Collective Deterrence. NSIP is a common fund that all member Nations contribute to and is intended to support investment directly related to "deterrence, defence and security, by supporting capability development and delivery, particularly on air, land and naval facilities, bulk fuel pipeline systems and storage, reinforcement, sustainment and enablement capabilities, core communications, information technology networks, satellite communications and readiness initiatives" (NATO, 2023). The Baltic Nations must heavily access this fund, which is set to grow from €1.7 billion in 2025 to €5.8 billion in 2030, particularly for their efforts to establish the Baltic Defence Line.

Public information suggests that Estonia has benefited from NSIP funding in past years for infrastructure improvements at Ämari Air Base, the NATO Force Integration Unit in Tallinn, the NATO Cyber Range, the Tapa military camp, and the Defence Forces central training area (Kaitseministeerium, 2025). However, for the Baltic to sustain a commitment to the new NATO regional plans, as they are three of the most vulnerable nations on NATO's eastern flank, their collective benefit from the NSIP must outweigh their collective contribution.

NSIP's investment in reducing the cost of the Baltic Defence Line is wise for all involved. Deterrence by denial means strengthening the defensive posture on the eastern flank of NATO, and this project is estimated to cost the Baltic Nations € 900 million over the next 5 years. Committing funds from the NSIP to defer half or more of those costs would significantly unburden the defence budgets of these nations, particularly Latvia and Estonia. While such a commitment would significantly adjust NSIP priorities, ensuring sustained commitment to collective deterrence in Baltic societies is necessary.

EU Fiscal Reform: Making Defence Economically Viable. Another way to defer costs and sustain commitment involves the EU changing its regulations to exclude defence spending from deficit calculation. Last year, in an update to its fiscal regulations, the EU adopted policies that affirmed its long-held rules on member nations maintaining a deficit of 3% or less of GDP and, if exceeded, for governments to implement plans to reduce the deficit to 1.5% (EU Press Release, 2024). Speaking at the Munich Security Conference in mid-February 2025, European Commission President Ursula von der Leyen said she would push for activating an "escape clause" to the deficit rule for defence spending (Sorgi, et al., 2025).

On March 19, 2025, the European Commission released its much-anticipated "White Paper for European Defence and the ReArm Europe Plan/Readiness 2030" (European Commission, 2025a). The White Paper included a "Communication - accommodating defence expenditure," outlining the procedure for activating the so-called "escape clause." Article 26 of Regulation (EU) 2024/1263 allows nations to request, through the European Council, to activate the escape clause when spending on defence, so long as three conditions are met.

The first condition is that “there are exceptional circumstances outside the control of the Member State” (European Commission, 2025b). The European Commission has already identified that Russia’s aggression satisfies this condition for all member states. The second condition is that “these exceptional circumstances have a major impact on the public finances of the Member State concerned” (European Commission, 2025b). The Baltic nations also satisfy this condition since this situation has caused them to double their defence spending effectively, and they are preparing for increased taxes or austerity measures to stay within the accepted EU guidelines for fiscal responsibility. The third condition is that “the deviation from the net expenditure path set by the Council does not endanger fiscal sustainability over the medium term” (European Commission, 2025b).

For this third condition, the Commission offers several guidelines. If a member state is authorised to use the “escape clause,” the Commission will allow for unpenalized deviation from the 3% deficit threshold that can be attributed to an increase of 1.5% in spending in GDP annually through 2028 (European Commission, 2025b). However, the Commission expressed reservations about approving the escape clause if the member state exceeded 60% of the national debt compared to GDP (European Commission, 2025b). Estonia’s national debt averaged 24% last year (CEIC Data, 2025a), Lithuania averaged 38% last year (CEIC Data, 2025b), and Latvia had the highest debt of the Baltic nations, averaging 47% (CEIC Data, 2024). This means all three Baltic countries are eligible for the “escape clause” approval and should apply as soon as possible.

While the escape clause is controversial in fiscally conservative states like Germany and Sweden (Sorgi, et al., 2025), it helps encourage smaller states and states already indebted to borrow more money to invest in defence. However, sustaining such a proposal must be more than an emergency “escape clause.” Instead, it ought to be voted on by the members of the European Parliament and accepted as a standard practice for all member nations to avoid counting defence spending toward their deficit. This will allow nations to buy what is needed to defend their national interests and uphold their NATO obligations while avoiding austerity measures or tax increases, which would challenge a nation’s ability to sustain such a commitment indefinitely.

Demographic Decline and the Future of Baltic Security. Another long-term problem facing the Baltic nations and most of Europe is demographic issues related to population decline and ageing. “The UK Ministry of Defence identifies 'Demographic Pressures' as its number two driver of global change in the 7th edition of Global Strategic Trends, citing population growth in parts of the developing world and population decline and ageing in the Western world as cause for alarm (UK Ministry of Defense, 2024). Demographic decline and an ageing population in the Baltic nations will acutely affect the security sector in these small nations as the available military-age population shrinks, and an ageing population stresses funding for military projects” (Ryan, 2025).

All three Baltic nations have had policies in place for a decade or more to reduce emigration and increase immigration, including progressive parental leave policies, “baby bonuses,” and tax incentives, which have failed to meet the desired goals of retaining young talent and suffer from the unfortunate reality of an untenable political environment for non-European migration to the EU. Demographic decline is inevitable in the Baltic, and governments must convince their citizens that migration is in the best interest of each nation to fund these necessary initiatives that support long-term viability and security.

According to the United Nations (UN), “international migration can have a positive impact on the demographic outlook of receiving countries by delaying or lessening the extent of population ageing and by slowing or averting population decline” (UN DESA Publications, 2023). The UN also notes that migrant workers often represent a substantial portion of the labour force in countries experiencing demographic decline and substantially improve the economic outlook in these declining nations (UN DESA Publications, 2023). The UN also notes, however, that nations that experience high volumes of irregular migration tend to face undue stress on their societal conditions, which impacts the popularity of these policies (UN DESA Publications, 2023).

As proposed by Ratzin and Kahanec in “A Sustainable Immigration Policy for the EU,” policies must more “effectively and selectively manage immigration based on the employability potential of the immigrant, combined with more attention to integration, and stricter measures to fight discrimination" (Ritzen & Kahanec, p 155, 2017). According to the most recent surveys on the popular opinion of migration in the Baltic, only 33% of Estonians find immigration useful (European Commission, 2016). Latvians allegedly have a negative opinion of immigration, but are generally favourable to an economic rationale for migration (Kaprāns, et al., 2021), and Lithuania supports non-Ukrainian immigration to the country at about 40% (IOM Lithuania, 2024). It will again require effective political communication of these measures to improve public opinion, and it would be wise to tie such measures to defence and security while being mindful of the societal disruption these policies can have.

It is also vital to develop incentives to attract immigrants wanting to work and stay in the Baltic region rather than moving west to more affluent European societies for economic opportunities. This will require the Baltic nations to adopt policies favouring emerging tech industrial investment in their countries and multilateral engagements with countries like India, which is experiencing significant growth in its middle-class and working-age population but struggling to provide a reliable infrastructure for its emerging technology industry. Attracting these types of companies to set up a base of operation in the Baltic may also encourage young native-born citizens to remain and slow emigration from the region.

From Urgency to Endurance: The Baltic Path to Sustainable Defence

> "What we invest in defence is how we value our defence. And for the past few decades, we haven't put a high enough price on it. We must spend more" (European Commission, 2025c).
>
> -- Kaja Kallas, High Representative for Foreign Affairs and Security Policy
> Vice-President of the European Commission

> "Europe can no longer afford to be a bystander in its security. We must take our defence into our own hands, reinforcing our commitments to collective security and standing firm against those who seek to challenge our sovereignty" (European Commission, 2025c).
>
> --Andrius Kubilius, Commissioner for Defence and Space

The quotes above, taken from two of the European Commission's top officials, who happen to be respectively Estonian and Lithuanian, highlight the urgent and critical importance of defence spending in Europe. They also convey how important it is for politicians to speak with one voice concerning the money that must be spent on the collective defence of Europe.

Balancing Threats and Burdens. The fact that the Baltic nations have such an outsized impact on the discourse at the European Commission is encouraging for the sustainment of these policies in the short to mid-term. Still, long-term sustainment must be the goal, particularly for the Baltic nations that face an indefinite threat from the east. To that end, the Baltic nations must collaborate with like-minded nations on Europe's eastern flank to do what international relations scholar Stephen Walt calls "balancing" in opposition to the principal danger (Walt, 1985).

In this case, a balancing strategy for the Baltic nations has two meanings. The first is against the Russian threat, which satisfies Walt's four historical prerogatives of aggregating power, proximity to the threat, offensive capability, and offensive intentions (Walt, 1985). By balancing with each other and like-minded nations, the Baltic can create economies of force by buying offensive capability together, as NATO Secretary General Mark Rutte suggested. They can more readily demonstrate that capability in the region.

The second way that the Baltic nations balance is in the European Community. The proximity they share to the threat and their increased influence in the European Union allows them to influence the dialogue and convince larger and more economically powerful nations that are less proximal to the threat to help the Baltic nations defer the cost of their defensive purchases by encouraging more substantial European investment in capability on the Eastern flank.

The burden sharing achieved through a combination of increased NATO common fund investment and more permanent adjustments to European regulation that stifle defence investment will allow the Baltic nations the ability to sustain their commitment to security and defence investment for the long term by putting less of a burden on the citizens of these small nations.

Endurance Through Integration and Strategic Alignment. While visiting the German Council on Foreign Relations in March 2025, a Russian defence expert relayed to the author that if Russia were to withdraw from its military commitment in Ukraine, he estimates that they could credibly threaten the Baltic nations with armed attack in a matter of weeks or months (DGAP Expert, 2025). The investments the Baltic nations intend to make are urgent and necessary, but Russia has the luxury of dictating the timetable and terms of such a conflict. This allows Russia to wait until the populations in the Baltic nations become weary of the cost, they incur to protect against a threat that has not yet materialised.

For this reason, the Baltic nations must take a longer view of their security by instituting and advocating for policies now that will have less of an impact on the public perception of such security measures. Politicians in the Baltic nations must convince their citizens that defence spending and capability acquisition are as critical as membership in the NATO alliance. A way to accomplish this is to connect defence spending to the more popular notion of the US and NATO as security guarantors. Baltic Politicians can point to reports that in 2025, the US presidential administration is considering “favouring NATO members that spend a set percentage of their GDP on defence” (BNS, 2025b).

They must also look more holistically at their societies and persuade their populations that demographic issues will compound Baltic economies in the coming decades, affecting the sustainability of their capability acquisition and filling their military ranks. Finally, the Baltic nations must balance with countries in similar security situations to influence sustained large-scale reform in Europe and encourage long-term investment in defence. In this way, the Baltic nations will get *more bang for their buck*.

Bibliography

Becker, Jordan. 2017. Clearing the Air on Transatlantic Burden-Sharing, Part III: Let’s Turn to Data. War on the Rocks. Online. 14 June 2017. Available from: https://warontherocks.com/2017/06/clearing-the-air-on-transatlantic-burden-sharing-part-iii-lets-turn-to-data/ [Accessed 28 February 2025].

BNS. 2024. Lithuania should boost defence budget to 4% of GDP – minister. Lrt.lt. Online. 16 September 2024. Available from: https://www.lrt.lt/en/news-in-english/19/2360807/lithuania-should-boost-defence-budget-to-4-of-gdp-minister [Accessed 2 March 2025].

BNS. 2025a. Lithuania's leaders agree on 5.5% GDP military spending. lrt.lt. Online. 17 January 2025. Available from: https://www.lrt.lt/en/news-in-english/19/2462751/lithuania-s-leaders-agree-on-5-5-gdp-military-spending [Accessed 16 March 2025].

BNS. 2025b. Rubio reaffirms US commitment to Baltic security in meeting with ministers. lrt.lt. Online. 25 March 2025. https://www.lrt.lt/en/news-in-english/19/2521118/rubio-reaffirms-us-commitment-to-baltic-security-in-meeting-with-ministers [Accessed 17 April 2025]

CEIC DATA. 2024. Latvia Government Debt: % of GDP, 2000 – 2025. Online. 2024. Available from: https://www.ceicdata.com/en/indicator/latvia/government-debt--of-nominal-gdp [Accessed 21 March 2025].

CEIC DATA. 2025a. Estonia Government Debt: % of GDP, 2000 – 2025. Online. 2025. Available from: https://www.ceicdata.com/en/indicator/estonia/government-debt--of-nominal-gdp [Accessed 21 March 2025].

CEIC DATA. 2025b. Lithuania Government Debt: % of GDP, 2000 – 2025. Online. 2025. Available from: https://www.ceicdata.com/en/indicator/lithuania/government-debt--of-nominal-gdp [Accessed 21 March 2025].

Česėkaitė, Ditė. 2024. Vyriausybė pritarė atgasymo įgyvendinimo priemonėms. Alkas.lt. Online. 1 August 2024. Available from: https://alkas.lt/2024/08/01/vyriausybe-pritare-karinio-kontrmobilumo-igyvendinimo-priemonems/ [Accessed 6 November 2024].

CSB Official Statistics of Latvia. 2024. Population by ethnicity in regions, cities, municipalities, towns, neighbourhoods and densely populated areas at the beginning of year. Online. 2024. Available from: https://data.stat.gov.lv/pxweb/en/OSP_PUB/START__POP__IR__IRE/IRE071/table/tableViewLayout1/ [Accessed 20 October 2024].

DGAP Expert, (Chatham House Rules). 2025. DGAP Presentation to Higher Command Studies Course. 14 March 2025.

ERR. 2024. Government reaches agreement on tax changes. ERR. Online. 17 September 2024. Available from: https://news.err.ee/1609462648/government-reaches-agreement-on-tax-changes [Accessed 3 March 2025].

ERR NEWS. 2024. Estonia to build 600 bunkers along Russian border. ERR. Online. 19 January 2024. Available from: https://news.err.ee/1609227386/estonia-to-build-600-bunkers-along-russian-border [Accessed 17 October 2024].

EU Press Release. 2024. New EU fiscal rules approved by MEPs | News | European Parliament. Online. 23 April 2024. Available from: https://www.europarl.europa.eu/news/en/press-room/20240419IPR20583/new-eu-fiscal-rules-approved-by-meps [Accessed 18 March 2025].

European Commission. 2016. European Social Survey: Attitudes of Estonians towards immigrants | European Website on Integration. Online. 3 May 2016. Available from: https://migrant-integration.ec.europa.eu/library-document/european-social-survey-attitudes-estonians-towards-immigrants_en [Accessed 21 March 2025].

European Commission. 2025a. Commission unveils the White Paper for European Defence and the ReArm Europe Plan/Readiness 2030. European Commission - European Commission. Online. 19 March 2025. Available from: https://ec.europa.eu/commission/presscorner/detail/en/ip_25_793 [Accessed 21 March 2025].

European Commission. 2025b. Accommodating defence expenditure | Defence Industry and Space. Online. 19 March 2025. Available from: https://defence-industry-space.ec.europa.eu/document/a57304ce-1a98-4a2c-aed5-36485884f1a0_en [Accessed 21 March 2025].

European Commission. 2025c. Commission unveils the White Paper for European Defence and the ReArm Europe Plan/Readiness 2030. European Commission - European Commission. Online. 19 March 2025. Available from: https://ec.europa.eu/commission/presscorner/detail/en/ip_25_793 [Accessed 21 March 2025].

IOM Lithuania. 2024. IOM Lithuania: Ukrainians are the most favoured migrants in Lithuania. Online. 22 November 2024. Available from: https://lithuania.iom.int/news/iom-lithuania-ukrainians-are-most-favoured-migrants-lithuania-0 [Accessed 21 March 2025].

Kaitseministeerium. 2024a. Defence budget. Online. 2024. Available from: https://kaitseministeerium.ee/en/objectives-activities/defence-budget [Accessed 3 March 2025].

Kaitseministeerium. 2024b. Public Opinion on National Defence. Online. 18 October 2024. Available from: https://www.kaitseministeerium.ee/sites/default/files/public_opininon_and_national_defence_2024_spring.pdf.pdf [Accessed 18 October 2024].

Kaitseministeerium. 2025. Allied Contribution. Estonian National Defence Development. Online. 2025. Available from: https://riigikaitseareng.ee/en/allied-contribution/ [Accessed 18 March 2025].

Kaprāns, Mārtiņš; Andris Saulītis; Inta Mieriņa. 2021. Attitudes towards immigration in Latvian society. Migration ⇄ LV. Online. 7 December 2021. Available from: https://migracija.lv/en/publication/2021-attitudes-towards-immigration-report/ [Accessed 21 March 2025].

Kiisler, Indrek. 2024. Minister: New NATO plan may hike Estonia's defense spending to 5 percent. ERR. Online. 2 September 2024. Available from: https://news.err.ee/1609441616/minister-new-nato-plan-may-hike-estonia-s-defense-spending-to-5-percent [Accessed 2 March 2025].

LRT News. 2024. Lithuania to get EU funding for Russia border security – minister. lrt.lt. Online. 25 July 2024. Available from: https://www.lrt.lt/en/news-in-english/19/2326345/lithuania-to-get-eu-funding-for-russia-border-security-minister [Accessed 18 October 2024].

Mazarr, Michael J. 2018. Understanding Deterrence. RAND. Online. 19 April 2018. Available from: https://www.rand.org/pubs/perspectives/PE295.html [Accessed 3 March 2025].

Milevskl, Lukas. 2024. The Baltic Defense Line - Foreign Policy Research Institute. Online. 2 February 2024. Available from: https://www.fpri.org/article/2024/02/the-baltic-defense-line/ [Accessed 17 October 2024].

Ministry of Defence Estonia. 2024. Baltic countries to build defensive installations on their borders | Kaitseministeerium. Online. 2024. Available from: https://www.kaitseministeerium.ee/en/news/baltic-countries-build-defensive-installations-their-borders [Accessed 17 October 2024].

Ministry of Defence Latvia. 2025. Budžeta infografika (2025. gadam) ENG.jpg (1241×4147). Online. 2025. Available from: https://www.mod.gov.lv/sites/mod/files/document/Bud%C5%BEeta%20infografika%20(2025.%20gadam)%20ENG.jpg [Accessed 3 March 2025].

MOD Military Public Affairs Department. 2025. Next year's Defence funding must be increased to 4% of GDP | Aizsardzības ministrija. Online. 20 February 2025. Available from: https://www.mod.gov.lv/en/news/spruds-next-years-defence-funding-must-be-increased-4-gdp [Accessed 2 March 2025].

NATO. 2014. Wales Summit Declaration issued by NATO Heads of State and Government (2014). NATO. Online. 5 September 2014. Available from: https://www.nato.int/cps/en/natohq/official_texts_112964.htm [Accessed 16 October 2024].

NATO. 2023. The 2024-2028 Common Funding Resource Plan. NATO. Online. 31 July 2023. Available from: https://www.nato.int/cps/en/natohq/official_texts_217756.htm [Accessed 18 March 2025].

NATO. 2024a. Defence expenditures and NATO's 2% guideline. NATO. Online. 18 June 2024. Available from: https://www.nato.int/cps/en/natohq/topics_49198.htm [Accessed 16 October 2024].

NATO. 2024b. "To Prevent War, NATO Must Spend More" - Speech by NATO Secretary General Mark Rutte at the Concert Noble, Brussels. NATO. Online. 12 December 2024. Available from: https://www.nato.int/cps/en/natohq/opinions_231348.htm [Accessed 2 March 2025].

NATO. 2024c. NATO Press Release - Defense Expenditures 2024. Online. 2024. Available from: https://www.nato.int/nato_static_fl2014/assets/pdf/2024/6/pdf/240617-def-exp-2024-en.pdf [Accessed 21 October 2024].

Posaner, Joshua; Laura Kayali, Julius Brinkmann; Oliver Noyan. 2025. Europe splits on Trump's call to dramatically boost defense spending. POLITICO. Online. 8 January 2025. Available from: https://www.politico.eu/article/donald-trump-tells-allies-spend-5-percent-gdp-defense-nato/ [Accessed 28 February 2025].

Ritzen, J., Kahanec, M. 2017. A Sustainable Immigration Policy for the EU. Ritzen, J. (eds) A Second Chance for Europe. Springer, Cham. 2017, 155-181.

Ryan, Kevin M. 2024. The New 'Baltic Way': Assessing the Baltic Defensive Line Concept - Foreign Policy Research Institute. Online. 13 December 2024. Available from: https://www.fpri.org/article/2024/12/the-new-baltic-way-assessing-the-baltic-defensive-line-concept/ [Accessed 8 April 2025].

Ryan, Kevin M. 2025. Position Paper - Bandwagoning for Demographic Security in the Baltic States. 6 February 2025. HCSC, Baltic Defence College.

Sorgi, Gregorio; Antoaneta Roussi; Joshua Posaner. 2025. Von der Leyen demands trigger of emergency clause to massively boost defense spending. POLITICO. Online. 14 February 2025. Available from: https://www.politico.eu/article/von-der-leyen-proposes-triggering-clause-to-massively-boost-defense-spending/ [Accessed 18 March 2025].

Strashkulych, Anhelina. 2024. Old men belong here. How Ukrainian Armed Forces have become 40+ age army and whether lowering mobilisation age will affect combat capability. Ukrainska Pravda. Online. 2024. Available from: https://www.pravda.com.ua/eng/articles/2024/05/16/7455980/ [Accessed 18 March 2025].

UK Ministry of Defense. 2024. Global Strategic Trends: Out to 2055. GOV UK. Online. 27 September 2024. Available from: https://www.gov.uk/government/publications/global-strategic-trends-out-to-2055 [Accessed 12 February 2025].

UN DESA Publications. 2023. UN DESA Policy Brief No. 146: Why safe, orderly and regular migration matters for sustainable development. Online. 4 January 2023. Available from: https://desapublications.un.org/policy-briefs/un-desa-policy-brief-no-146-why-safe-orderly-and-regular-migration-matters [Accessed 21 March 2025].

Walt, Stephen M. 1985. Alliance Formation and the Balance of World Power. International Security. 1985. Vol. Vol. 9, no. 4, p. 3. DOI 10.2307/2538540.

World Bank. 2023. Military Expenditure (Current USD) and (% GDP), 2023. World Bank Data. Online. https://data.worldbank.org/indicator/MS.MIL.XPND.CD?end=2023&locations=US-EE-LV-LT&start=2023&view=chart [Accessed 17 April 2025].

LTC Erki Soo. Will Artificial Intelligence (AI) make human strategic planning (in logistics) obsolete?

Introduction

According to the study, the rise and active usage of artificial intelligence are expected to boost the global economy from $1.2 trillion in 2024 to $4.9 trillion by 2030. (Fried, 2024). This trend raises concerns about whether AI could eventually replicate or outweigh human strategic planning, especially in domains reliant on complex judgment and ethics. Moreover, it raises the question of whether AI can learn and/or replicate human traits, especially those unique to us, such as empathy, emotion, feelings, ethics, creativity, and consciousness.

Two key drivers frame the research paper: necessity due to the changing security environment and opportunity due to the rise of emerging technology.

The first reason for addressing this topic is necessity. The evolving security environment in Europe and the Baltic Sea region demands innovative approaches to managing rapid capability developments and increasing defence expenditures. However, integrating and implementing new military capabilities requires additional human resources. All three Baltic states have faced significant demographic challenges over the past decade, including declining and ageing populations (Varpina, 2018). This creates a critical challenge: recruiting and sustaining a capable military force when the available workforce is shrinking.

The second is that the opportunity presented by emerging technologies, such as artificial intelligence, could help address this challenge by enhancing operational efficiency, automating certain military functions, and reducing the overall demand for human personnel. AI has the potential to support decision-making, optimise logistics, and even perform tasks that currently require significant human involvement, making it a valuable tool for future defence strategies.

This raises a critical question: can AI be effectively integrated to support strategic planning without replacing the human element?

This research paper argues that although artificial intelligence continues to improve and develop and reshaping decision-making across all levels, it will not render human strategic planning obsolete, primarily due to its inherent limitations in possessing unique human traits such as empathy, an ethical and moral compass, as well as strategic intuition – qualities and attributes essential for high-level planning and decision-making. Rather than replacing humans, in the author's opinion, it will act as a force multiplier by enhancing analysis, enabling faster and data-driven decision making.

This research paper is structured into three chapters. The first chapter provides a brief historical background of artificial intelligence, especially its evolution and definition. This will help establish a framework for understanding how nations should approach and handle AI today or in the near future. The second chapter elaborates on the usage of AI in the civil sector, with a clear focus on logistics, highlighting best practices and innovations that may be relevant to military logistics. It also explores principles and policies defined by the nation or multinational organisations like the EU and NATO. The third chapter will examine the role of AI in military logistics, discussing how AI can support and enhance decision-making and resource management in military operations.

1. Historical and conceptual foundation of artificial intelligence in a strategic context.

This chapter provides background information on when humankind first began discussing artificial intelligence, the ideas surrounding AI, and its evolution. It will also elaborate on how AI is defined and what could be the central philosophical driver of autonomous systems. It is relevant to understand, while using AI in a supporting role for decision-making, what drove humankind to develop AI applications and is driving the development of robots.

Before presenting how AI is used by various nations and organisations nowadays, it is essential to lay the historical foundation to understand how AI has evolved. 2500 years ago, in Greek mythology, an automated giant named Talos, fabricated by Hephaestos, who was a god of innovation and technology, guarded the Greek island of Crete (Mayor, 2024). As it was an autonomous system that could understand its surroundings to protect the island, it has been argued that this aligns with the definition of a robot. Although the roots of AI lead back to antiquity, we can say that the beginning was in 1956, when, during a study program at Dartmouth College, the goal was stated to explore how machines understand and use language, form concepts, solve problems for humans, and even improve themselves over time (Russell, 2019). We can say that already 2500 years ago, humankind was seeking something that could fulfil specific tasks that humans couldn't accomplish.

Alan Turing, in 1951, during a lecture in Manchester, mentioned that once the machine thinking method had started, it wouldn't take long to outstrip weak humans (Russell, 2019). In this sense, he is right, as the development of machines that support humans has progressed enormously in the last few decades and has taken over many jobs. And today, as we have begun to use AI widely, it will take over many jobs.

However, before proceeding with the research, it should first be understood and defined what AI is. It helps us to better understand for which purpose AI is developed and used nowadays, and what other fields it could be effectively utilised in. The European Parliament has defined AI as a machine's ability to show human traits like reasoning, learning, planning, and creativity (European Parliament, 2023). Another example is provided by the United States Air Force, where artificial Intelligence refers to 'the ability of machines to perform tasks that normally require human intelligence – for example, recognising patterns, learning from experience, drawing conclusions, making predictions, or taking action – whether digitally or as the smart software behind autonomous physical systems' (The United States Air Force, 2019). As previously indicated, AI has been defined differently, but the core principles remain similar. Another critical aspect to consider is that AI is also used in autonomous systems with a physical body or shell, making them a type of robot, especially when speaking of automated systems led by AI. At the beginning of the 1950s, American science fiction writer Isaac Asimov stated the three laws of robotics:

1. ‘A robot may not injure a human being or, through inaction, allow a human being to come to harm.
2. A robot must obey the orders given to it by human beings except where such orders would conflict with the First Law.
3. A robot must protect its own existence as long as such protection does not conflict with the First or Second Laws’ (Bales, 2024).

AI has a long history and has evolved like the rest of technology. Today, the primary role is supporting and enhancing humans, rather than replacing them. Developing AI and integrating AI with autonomous systems also requires considering the principles of Asimov's three laws. Different AI definitions and ethical guidelines show that AI is a tool, created and guided by humans, led by human values and operated under human supervision. In the author's opinion, it must be remembered that AI continues to progress and evolve, while also considering its limitations. With this understanding, we can dive into how AI transforms modern logistics, particularly in the civilian sector, where its innovations will provide valuable insights for military applications.

2. The use of artificial intelligence in civil and military logistics today.

The second chapter explains how AI is currently utilised in the civil sector for decision-making, focusing on logistics. It begins by discussing ethics and the use of AI in decision-making, as the ethics of AI are a vital aspect of using it. This will be followed by examples of how AI is applied in civil logistics. It will also explain how NATO and other militaries have defined their policies and how they have been aligned with national-level principles.

The role of AI is to facilitate or support human decision-making, ensuring that our values are considered and can be justified in accordance with our morals. However, when starting to use AI in decision-making, it is also crucial to understand its moral and ethical implications, as the ultimate responsibility for making decisions lies with the decision-maker, and we cannot delegate this responsibility to AI.

It is essential to note that transparency, accountability, and fairness are fundamental when developing and integrating AI into decision-making processes. These ethical traits will become even more crucial in a military context, where decisions —often involving life or death, national security, or regional stability —will be at stake. The lack of transparency in AI raises questions and concerns regarding explainability and trust. AI, as a black box, making decisions in a military operation, could have biases or overlook certain aspects that a human would intuitively engage with or intervene in. That is why keeping ethical guidance and human responsibility at the centre while using AI is essential.

Jessica Woodgate and Nirav Ajmeri from the University of Bristol (UK) have analysed human values and moral considerations, which should be considered as part of the AI systems in support of decision-making and provided six main ethical principles:

1. Transparency and explainability, meaning that the system should operate in a manner that is understandable to users.
2. Accountability, in the sense that precise mechanisms must be established to hold AI and its developers accountable for the outcomes of AI-driven decisions.
3. Fairness and non-discrimination decisions, where AI makes impartial decisions that avoid biases.
4. Privacy and data protection are crucial for AI systems.
5. Human oversight and judgment must be incorporated into critical decision-making to address all relevant considerations adequately.
6. Safety and security for the users must be granted to prevent harm and not compromise their integrity (Woodgate, 2024).

To align AI development-related procedures and prevent the misuse of AI, it is essential to develop policies and principles governing the use of AI. In the era of rapid development of emerging technologies, it is imperative that nations and organisations, especially multinational organisations, develop their strategies and policies in various areas of AI usage. For instance, the European Union Ethics Guidelines for Trustworthy AI describe four principles:

1. ‘Respect for human autonomy.
2. Prevention of harm.
3. Fairness.

4. Explicability' (Kung, 2020).

The same principles and guidelines apply to large corporations leading the development of computing and AI. The COE of Microsoft has defined six goals or principles that should be considered by industry and society:

1. AI should be developed to support and empower humans, not replace them.
2. AI working system should be visible and understandable.
3. Efficiency gains from AI should not come at the cost of human dignity.
4. AI systems must handle personal data with discretion and care.
5. Humans must be able to take responsibility for AI outcomes.
6. Bias must be actively identified and reduced in AI systems (Shaldbolt, 2024).

Understanding AI-related ethical considerations and recognising that nations and organisations are investing significant effort in developing AI-related policies, it can be analysed how logisticians in complex environments utilise AI. The primary reason for the rapid development of AI is that it enables specific tasks to be completed more efficiently, accurately, and at a lower cost. This is also one of the reasons why AI is very actively used in logistics. The civil sector has already demonstrated that AI can increase logistical productivity and efficiency by over 40%, especially in high-volume operations such as maritime shipping (Transmetric, 2023). This has been achieved through AI's ability to forecast demand, optimise routes and dynamically allocate resources. In military logistics, similar AI applications could support theatre-level supply chain management, avoid equipment shortages and reorganise or re-plan resupply operations, especially in an environment where time and adaptiveness are critical.

Maritime transport is considered the backbone of global trade and the economy, as 50% of world trade in value is facilitated by maritime transport (Verschuur, 2022). This again places a significant amount of stress and focus on port operations and logistics, as over 80% of world trade by volume and over 70% by value is conducted via these means of transport (Sima, 2024). According to a study that utilised an AI-based port logistics application during a port logistics simulation, around $7.3 million in extra direct profit could be gained yearly, along with a 79% improvement in ship accuracy, generating environmental benefits for the port (Sima, 2024). Although it was a simulation, actual data were used to explore the AI solution for port operations, including predicting estimated arrival time, monitoring and optimisation of port operations, fuel consumption, and various risk assessments. These findings show that AI-driven simulations can play a valuable role in improving both the accuracy and long-term reliability of decision-making in port logistics. Another area where AI can be effectively utilised is warehousing. The integration of AI and robots, or automated systems, has led to significant improvements in warehousing, as AI-led autonomous systems can efficiently sort, pick, pack, and organise inventory, thereby making the order process faster (Muynck, 2023).

Artificial intelligence (AI) is already transforming how we manage logistics daily. For example, it could help cargo ships determine the quickest routes and enhance warehouse operations efficiency. These advancements offer insight into how similar applications could also enhance military logistics. Speed, ability to handle and analyse a large amount of data and capacity to make decisions independently are the main features of AI. However, ethical concerns and technical limitations need to be solved. This is why human judgment and decision-making are essential for using AI effectively and responsibly.

This brings us to an important question: how is AI being adapted for military logistics, where the stakes are much higher, involving lives, national security, and critical strategic decisions?

In July 2024, a study was published investigating and analysing the use of AI applications in supply chain optimisation. The outcome was that the usage of AI applications contributed to a 28% reduction in resource consumption and a 15% decrease in carbon emissions (Kelly, 2024). This shows significant potential for applying AI in supply chain management.

By analysing the use of AI in logistics across various functions, another field where AI can be effectively applied is transportation. In the United States, trucks are approximately 30% empty on average, wasting time and fuel, whereas the use of AI applications has reduced this to 10-15% (Burnham, 2024). Like other logistical areas, AI has proven effective in the medical and healthcare fields. The digitalisation of medical records enables faster and more informed decision-making, and robots led by

AI have the potential to become more accurate and reliable surgeons than humans (Tegmark, 2018). In conclusion, the role of AI in logistics and its applications are limitless, as it can be effectively utilised in every aspect of logistics.

AI has enabled us to utilise it as a helpful tool that should be incorporated into logistics to make the supply chain more sustainable and eco-effective. However, like many other tools, AI also has its challenges, drawbacks, limitations, and barriers, such as:

- Data availability, quantity, and quality.
- High implementation and sustainment costs.
- Policies and regulations are required, lack of transparency and AI could be unethical and unpredictable.
- There are no standards defined for AI-driven logistics.
- Networks and different systems to be interconnected is a challenge (Shawon, 2025).

These challenges are akin to real-time problems companies face when integrating AI applications into their daily logistics and supply chains. Kenneth Payne explores in his book, ‘I, Warbot,’ how AI might influence the future of warfare, drawing on Margaret Boden’s taxonomy of creativity theory, which categorises creativity into combinatory, exploratory, and transformative forms. He suggests that AI advances along this spectrum, from combinatory now to transformational creativity in the future, as its autonomy and unpredictability will grow, making AI harder to control and understand its decisions (Payne, 2021). Based on Payne’s explanations and examples of three AI creativities, it can be said that military strategic planning is being shaped but not made obsolete, as humans still set broader objectives and ethical limits. However, considering the moral principles, the EU’s ethical guidelines, and the military environment, such an evolution of AI, which is unpredictable and autonomous, may pose a significant risk to humans. It must also consider the risks associated with AI supporting decision-making at every level. However, risks must be assessed and mitigated, and AI systems should be built based on human needs and agreed-upon ethical principles. This also means that humans will shift from a planning role to an observer or goal-setting role.

It has been decades since civil society has begun to utilise AI for various purposes, as explored in the previous chapter, highlighting its benefits, as well as its limitations and threats. In 1991, the US military started to use an AI application called DART (Dynamic Analysis and Replanning Tool) to aid decision support for US Commands and saved millions of dollars after beginning to use it (Military Embadded Systems, 2019). However, AI has developed significantly over the past three and a half decades, and its usage has grown substantially worldwide, particularly in the military. Emerging technologies like AI serve as a force multiplier in the military by analysing large amounts of data, enhancing operational and combat effectiveness, and supporting decision-making while reducing human workload and costs. There is no doubt that, just as civilian logisticians use AI, it can also be effectively utilised in military logistics to enhance logistics functions through artificial intelligence. However, the military has its unique peculiarities, compared to the civil world, which require, to some extent, a different approach and AI applications. In May 2024, IBM hosted an annual conference for senior defence and intelligence leaders to discuss how AI could support decision-making across the defence, and the main conclusions were:

- AI will enhance decision-making by making decisions faster and more accurately, increasing battlefield effectiveness.
- AI usage in defence is mostly in its early stages, as it has been agreed that human oversight must be maintained, especially in lethal operations.
- AI is used when time-critical decisions need to be made, allowing for faster and more accurate decisions. However, it will not replace humans, as humans will make the final decision.
- Collaboration and partnership between stakeholders, including defence organisations, civil and academic partners, must lead to the development of AI (Keegan, 2024).

Ethical questions and principles related to AI have surrounded us for a long time and have become increasingly important, including in the military. That is why it is essential to define national and organisational policies and principles, and to agree upon ethical questions. During the same conference, four key takeaways were stated, which are essential, especially from the strategic leaders' perspective:

- The Importance of AI: It was agreed that AI will be the key to future military operations.
- Importance of data quality: Reliable and accurate data are crucial for effective AI applications, and it is critical to set priorities in data quality.
- Areas for development: AI holds significant potential in logistics.
- Collaboration and Education: Advancing AI in defence requires cooperation across sectors and investment in education (Keegan, 2024).

Large corporations, civilian companies, and senior military and governmental leadership have realised the necessity for policies and strategies defined at the national level. They will represent the primary principles for utilising AI applications, considering the ethical implications of this technology. In July 2019, Estonia's national artificial intelligence strategy 2019-2021 was approved by the Government of the Republic of Estonia, and the second update was made in 2021, when Estonia's National AI Strategy for 2022–2023 was released (Ministry of Justice and Digital Affairs, 2024). The main objective of the National AI strategy was to define and agree upon actions that the Estonian government must take to advance AI in both the private and public sectors, and align with EU-level strategies (Government of the Republic of Estonia, 2019). From the strategic leadership perspective and a logistical point of view, the Estonian National AI strategy has highlighted the following areas and activities to focus on:

- Implementing AI solutions in the private and public sectors.
- R&D (research and development) and education.
- Data is an enabler, where limited and poor data quality is a considerable limitation.
- A legal framework to guarantee that national laws and regulations align with those of the European Union and the Council of Europe, regulating the use of AI (Ministry of Economic Affairs and Communications, 2021).

These national strategies set the overarching framework for where and why AI applications should be used, both in the private and public sectors. Understanding national strategies supports developments at every level and guarantees alignment at a broader, EU-wide level. However, as important as alignment with EU policies is, it is equally important to align with other organisations, such as NATO.

On the 21st of October 2021, NATO's Defence Ministers agreed on an Artificial Intelligence strategy for the first time to outline how AI can be integrated into defence and security by setting standards according to international laws and NATO values (NATO, 2021). On July 10, 2024, NATO revised its AI strategy, building on the progress made with the previous strategy to significantly enhance NATO's AI readiness and, from a strategic leadership and decision-making perspective, the following updates were made:

- Integrating AI into the NATO Defence planning Process.
- Increased cooperation and interoperability among and between Allies, NATO partners, and industry in all fields (NATO, 2024).

The sequence of policy development is that companies developing AI applications initially raise the question. States then develop and implement policies in close cooperation with international organisations like the EU and NATO, as policies and principles must be aligned between states' organisations, serving as guidance for companies developing AI applications.

Nations have developed more detailed AI strategies based on the principles of NATO and the EU and national strategies for their national defence. Taking two examples from NATO: an EU member state, Estonia, and another NATO member but a non-EU state, the United States, with a focus on strategic decision-making and the role of AI in that process. The United States Department of Defense has been actively investing and developing AI-enabled systems for over six decades, culminating in the publication of its first national AI strategies in 2018, which was revised in 2020 and updated most recently in June 2023 to reflect evolving strategic priorities and technological advancements (Department of Defense, 2023). Another important aspect is that in 2018, following the development of the AI strategy, the Joint Artificial Intelligence Centre was established to execute all the activities necessary to implement the principles and policies outlined in the strategy (Sydney, 2018). It highlights the significance of AI-related developments in the US in terms of competing with Russia and China. Returning to the US AI strategy and the strategic environment, the focus area is on implementing the principles to enable leaders to make fast and well-informed decisions with the following outcomes and focus areas:

- 'Battlespace awareness and understanding.

- Adaptive force planning and application.
- Fast, precise, and resilient kill chains.
- Resilient sustainment support.
- Efficient enterprise business operation' (Department of Defense, 2023).

As stated in the US, the AI strategy also supports decision-making in the sustainment field. Similarly significant is the utilisation of AI applications for the Estonian Ministry of Defence, which has stated in its initial defence Artificial Intelligence strategy three main objectives:

1. Establishing direct military advantages by supporting decision-making, enhancing intelligence processing, and accelerating targeting.
2. Improving support services and logistics efficiency through a faster and more accurate analysis capability and reducing administrative burdens.
3. Strengthening the local defence industry through increased partnership between the Estonian Defence Forces (EDF) and the defence industry, driven by the development and application of defence AI (The Ministry of Defence of Estonia, 2025).

Having examined two national-level defence-focused policies, the author can emphasise similarities in the role of AI in decision-making and AI support for sustainment and logistics, both of which are key focus areas in these policies. This means that decision-making and sustainment are important areas where AI applications can be effectively utilised.

3. AI for a strategic leader in the military logistics field.

International organisations, such as the EU and NATO, and various nations have established national and defence-level policies to implement AI applications effectively. The next chapter focuses on the role of AI in military decision-making, with a specific emphasis on its support for logistics. It provides an overview of the potential advantages of AI integration in logistics, accompanied by real-life examples from different military organisations.

To structure the chapter the NATO logistics functions serve as a roadmap, outlining the following functions: supply, material, services, logistics information management, equipment maintenance and repair, movement and transportation, reception, staging and onward movement (RSOM), infrastructure engineering for logistics (IEL), medical support, contractor support and Host Nation Support (NATO HQ, 2012). However, command and control (C2) is an additional function or activity for commanders. As highlighted as a separate focus area in policies, the employment of AI in C2 will be explored further.

- Command and control

One of the key advantages of AI applications is their ability to collect, process and analyse large amounts of data from different sources, such as sensors, satellites, and intelligence systems, as well as connect different existing systems and databases to support better decision-making and streamline logistic operations (Lacroix, 2023).

- Supply

As AI can analyse vast quantities of data, an AI-driven predictive analytical application can be used for forecasting supply demands and verifying that the right equipment is in the right place at the right time (Lacroix, 2023).

- Material

In October 2024, the US Army's Data, Engineering, and Software division initiated a test using generative AI to streamline repetitive and time-consuming tasks, enhancing efficiency and improving information accuracy in acquisition processes. (U.S. Army, 2024).

- Equipment maintenance and repair

By utilising predictive AI applications, logisticians can anticipate when vehicle parts need replacement, enabling timely maintenance that reduces costs, enhances operational safety, and helps prevent unexpected breakdowns (Lacroix, 2023).

- Movement and transportation

AI applications can improve at reacting to unexpected events and changing conditions through automated planning and decision-making to reroute supplies and personnel automatically (Lacroix, 2023).

In addition to automated rerouting, integrating AI applications with autonomous systems in military transportation can work 24/7, ensuring that military operations won't be interrupted because of delays in logistics (Sander, 2024).

- Medical

In June 2024, an article in the Army University Press was published, analysing how AI applications can be effectively used by medics in the future battlefield with the following outcomes:

  - Increased volume of data to support clinical decision-making acutely, routinely, and emergently; incorporating AI will add limitless value by maximising soldiers' ability to return to duty and increasing survivability on and off the battlefield.
  - AI can be used to increase health protection through health surveillance and disease prevention programming by analysing data. AI can inform medical planning and identify potential health risks to populations and individuals.
  - AI can enhance treatment and hospital management by improving diagnostic accuracy, treatment plans, risk factor assessment, health communication, and healthcare administration.
  - AI can be used to increase the accuracy and efficiency of processing patient movement requests, as it can drastically shift the movement of patients, from initiating patient care, through providing definitive care (Worsham, 2024).

- Challenges and concerns

US Army logisticians have stated that integrating AI into logistics also has several concerns:

  - Relying too much on technology at the expense of human experiences and intuition, which are essential traits in complex situations.
  - Implementing AI is costly due to the need for infrastructure upgrades, software development, and ongoing maintenance.
  - AI applications are vulnerable to cyberattacks and adversarial manipulation.
  - There is also an ethical consideration, as using AI applications could lead to decisions that lack transparency.

- Lastly, the usage of AI applications in logistics could lead to a high number of workforce requiring retraining or even an increase in unemployment (Lacroix, 2023).

This chapter examined how international organisations, such as NATO and the EU, as well as various nations, integrate AI into military logistics and decision-making. Using NATO's logistics functions as a guide, the chapter highlights the practical benefits of AI across multiple areas, including supply, maintenance, transportation, and medical support, demonstrating how AI is helping militaries make faster and more accurate decisions. The chapter also discussed the role of AI in command and control (C2), where it connects systems and increases situational awareness. Different examples are summarised in this chapter to illustrate the use of AI in military logistics.
What emerges from this chapter is a clear pattern: AI has the potential to significantly enhance every logistical function within the military, from predictive maintenance to battlefield medical support. However, even as systems become more autonomous and interconnected, the author thinks that the role of human strategic leadership remains irreplaceable. AI may analyse data faster than any soldier ever could, but the human mind provides ethical context, operational judgment, and mission intent. As the military integrates and applies AI more deeply, the priority must be to ensure these tools support the commanders responsible for strategic outcomes.

Conclusion

In the era of emerging technology and shrinking demographics, this research aimed to analyse whether AI could render human strategic planning in logistics obsolete. The main argument proposed that although AI has significantly developed in decision-making, it cannot replace humans and their traits, such as empathy, creativity and ethical reasoning, which are essential in strategic planning.

The findings across the three chapters have consistently reinforced this thesis. The historical and conceptual overview in the first chapter revealed that while AI has advanced from myth to mainstream, its development has always been in the service of human needs. The second chapter provided an overview of how the civil sector is already effectively utilising AI applications in logistics, making it faster, cheaper, and more sustainable. However, even with effectiveness, human judgment and final decision-making remain. Human traits, like ethical oversight, accountability, and values, cannot be coded into algorithms. The third chapter explored how militaries apply similar technologies from equipment maintenance to battlefield medicine. Here too, AI offers real advantages. However, when it comes to decisions that affect lives and mission success, leaders and organisations agree that people, not machines, must take responsibility. AI can support decision-making, but it should never make decisions alone.

However, answering the research question is not straightforward. While AI is transforming logistics, it will not replace human strategic planning. Instead, AI will increasingly act as a powerful tool, increasing our decision-making speed, accuracy, and quality. From a leader's perspective, instead of making detailed plans, leaders will need to focus more on setting clear goals and guiding AI systems with a sense of ethical responsibility. Strategically, it is necessary to rethink what leadership looks like in the military and how organisations are structured.

At the same time, it is essential to recognise the study's limits. AI is evolving rapidly, so much of the existing research remains in development or is speculative. Understandably, information on real-world military use of A, especially anything classified, is hard to access. This study draws on publicly available sources, academic research, and policy documents, which may not fully reflect what is happening behind the scenes.

Recommendations

From a strategic level perspective, an important aspect of enhancing logistics with AI is the decision to analyse and find the benefits of integrating AI into military logistics, meaning to start utilising its potential as much as possible and reasonably.

Regional cooperation: as analysed, developing efficient AI applications is costly and may not be affordable for small states. Therefore, it is essential to cooperate and share in the development of AI, including costs, knowledge, and human resources. For instance, three Baltic States could establish a working group to develop a framework and a road map for implementing AI in military systems.

Enhanced NATO's role: NATO is the leading security alliance, with an AI strategy and emphasising cooperation. It should take the initiative within the alliance and initiate NATO-wide AI application development in logistics.

Investment in AI literacy: commanders and staff officers at all levels must receive training not only on how to use AI tools effectively, but also on understanding their limitations, biases, and the risks associated with overreliance on AI.

Integrate AI into doctrines and wargaming: AI must not remain a standalone innovation. Strategic planning exercises, doctrines, and simulations should incorporate AI applications into broader operational concepts and strategies.

Maintaining Human-in-the-Loop Systems: AI should be used as a support mechanism, especially in logistics planning and execution. Final decision-making authority must remain with human commanders to ensure legal and moral responsibility.

Preparing for disruption and adversarial use: military planners must include AI as a variable in threat assessments, considering both the opportunities AI provides and the challenges posed by adversaries using similar technologies.

Bibliography

Bales, Rebecca. 2024. History-Computer. *Asimov's Laws of Robotics: Everything You Need To Know.* [Online] History-Computer, 24 12 2024. [Cited: 25 03 2025.] https://history-computer.com/technology/asimovs-laws-of-robotics/.

Burnham, Kristin. 2024. MIT Sloan School of Management. *How artificial intelligence is transforming logistics.* [Online] 20 08 2024. [Cited: 25 03 2025.] https://mitsloan.mit.edu/ideas-made-to-matter/how-artificial-intelligence-transforming-logistics.

Department of Defence. 2023. Department of Defence. *Data, Analytics, and Artificial Intelligence Adoption Strategy.* [Online] 27 06 2023. [Cited: 30 03 2025.]

https://media.defense.gov/2023/Nov/02/2003333300/-1/-1/1/DOD_DATA_ANALYTICS_AI_ADOPTION_STRATEGY.PDF.

European Parliament. 2023. European Parliament. *What is artificial intelligence and how is it used?* [Online] European Parliament, 04 09 2023. [Cited: 05 03 2025.] https://www.europarl.europa.eu/topics/en/article/20200827STO85804/what-is-artificial-intelligence-and-how-is-it-used.

Fried, Ina. 2024. Axios. *AI will add $19.9 trillion to global economy by 2030, IDC predicts.* [Online] Axios, 17 09 2024. [Cited: 03 02 2025.] https://www.axios.com/2024/09/17/ai-global-economy-idc-2030.

Government of the Republic of Estonia. 2019. KRATT. *Estonia's national artificial intelligence strategy 2019-2021.* [Online] 25 07 2019. [Cited: 28 03 2025.] https://www.kratid.ee/en/_files/ugd/980182_8d0df96fd41145739dff2595e0ab3e8d.pdf.

Keegan, Michael J. 2024. IBM Centre for The Business and Government. *Exploring the Use of AI in Military & Defense Operations.* [Online] 06 06 2024. [Cited: 27 03 2025.] https://www.businessofgovernment.org/blog/exploring-use-ai-military-defense-operations.

Kelly, Alma. 2024. International Journal of Technology and Systems. *Impact of Artificial Intelligence on Supply Chain Optimization.* [Online] 31 07 2024. [Cited: 30 03 2025.] https://www.researchgate.net/publication/382846059_Impact_of_Artificial_Intelligence_on_Supply_Chain_Optimization.

Kung, Johnny. 2020. CIFAR. *Building an AI World: Report on National and Regional AI Strategies, 2nd Edition.* [Online] 30 05 2020. [Cited: 24 03 2025.] https://cifar.ca/wp-content/uploads/2020/10/building-an-ai-world-second-edition.pdf.

Lacroix, Everette Bud. 2023. U.S. Army. *Future of Army Logistics | Exploiting AI, Overcoming Challenges, and Charting the Course Ahead.* [Online] 1 08 2023. [Cited: 31 03 2025.] https://www.army.mil/article/267692/future_of_army_logistics_exploiting_ai_overcoming_challenges_and_charting_the_course_ahead.

Mayor, Adrienne. 2024. Engelsberg Ideas. *The Ancient Forerunner of AI.* [Online] 24 05 2024. [Cited: 16 03 2025.] https://engelsbergideas.com/notebook/the-ancient-forerunner-of-ai/.

Military Embadded Systems. 2019. Military Embadded Systems. *Military Embadded Systems.* [Online] Military Embadded Systems, 24 01 2019. [Cited: 27 03 2025.] https://militaryembedded.com/ai/machine-learning/artificial-intelligence-timeline.

Ministry of Economic Affairs and Communications. 2021. Kratid. *Estonia's National Artificial Intelligence Strategy or Kratt Strategy for 2022–2023.* [Online] 2021. [Cited: 28 03 2025.] https://www.kratid.ee/en/_files/ugd/980182_4434a890f1e64c66b1190b0bd2665dc2.pdf.

Ministry of Justice and Digital Affairs. 2024. AI. *Vision and strategies.* [Online] Ministry of Justice and Digital Affairs, 2024. [Cited: 28 03 2025.] https://www.kratid.ee/en/kratt-visioon.

Muynck, Bart De. 2023. Forbs. *The True Role Of AI In Logistics.* [Online] 17 08 2023. [Cited: 27 03 2025.] https://www.forbes.com/councils/forbestechcouncil/2023/08/17/the-true-role-of-ai-in-logistics/.

NATO HQ. 2012. NATO Archives Online. *NATO Logistics Handbook.* [Online] 11 2012. [Cited: 30 03 2025.] https://archives.nato.int/uploads/r/nato-archives-online/d/6/9/d690cd82d2a2db0250c3a0f41eacad794cc36129899c173662ada35924ddce6b/1490_NATO-Logistics-Handbook_2012_ENG_HR.pdf.

NATO. 2024. North Atlantic Treaty Organization. *Summary of NATO's revised Artificial Intelligence (AI) strategy.* [Online] 10 07 2024. [Cited: 30 03 2025.] https://www.nato.int/cps/en/natohq/official_texts_227237.htm.

—. 2021. North Atlantic Treaty Organization. *NATO releases first-ever strategy for Artificial Intelligence.* [Online] 21 10 2021. [Cited: 30 03 2025.] https://www.nato.int/cps/en/natohq/news_187934.htm.

Payne, Kenneth. 2021. *I, Warbot.* London : Hurst & Company, 2021.

Russell, Stuart. 2019. *Human Compatible.* USA : Viking, 2019. pp. 4-5.

Sander, Thomas. 2024. Medium. *The future of military logistics: how autonomous systems are shaping the battlefield of tomorrow.* [Online] 6 09 2024. [Cited: 31 03 2025.] https://medium.com/@thomasarnosander/the-future-of-military-logistics-how-autonomous-systems-are-shaping-the-battlefield-of-tomorrow-a9bc41b619fb.

Shaldbolt, Nigel, Hampson, Roger. 2024. *As if human.* London : Yale University Press, 2024.

Shawon, Reza E Rabbi, et al. 2025. Journal of Ecohumanism. *Designing and Deploying AI Models for Sustainable Logistics Optimization: A Case Study on Eco-Efficient Supply Chains in the USA.* [Online] 18 03 2025. [Cited: 27 03 2025.] https://arxiv.org/pdf/2503.14556.

Sima, Sunghyun, Kimb, Dohee, Parkc, Kikun, Baed, Hyerim. 2024. Artificial Intelligence-based Smart Port Logistics Metaverse for Enhancing Productivity, Environment, and Safety in Port Logistics: A Case. *arXiv.* [Online] Coronell University, 24 08 2024. [Cited: 27 03 2025.] https://arxiv.org/abs/2409.10519.

Sydney, J. Freedberg, Jr. 2018. Breaking Defense. *Joint Artificial Intelligence Center Created Under DoD CIO.* [Online] Breaking Defense, 29 06 2018. [Cited: 30 03 2025.] https://breakingdefense.com/2018/06/joint-artificial-intelligence-center-created-under-dod-cio/.

Tegmark, Max. 2018. *Life 3.0.* s.l. : Penguin Books, 2018.

The Ministry of Defence of Estonia. 2025. The Ministry of Defence of Estonia. *Defence Artificial Intelligence strategy for Estonia.* [Online] 23 03 2025. [Cited: 30 03

2025.] https://kaitseministeerium.ee/sites/default/files/defence_artificial_intelligence_strategy_for_estonia.pdf.

The United States Air Force. 2019. The United States Air Force. *Artificial Intelligence Annex to the Department of Defense Artificial Intelligence Strategy.* [Online] 2019. [Cited: 25 03 2025.] https://www.af.mil/Portals/1/documents/5/USAF-AI-Annex-to-DoD-AI-Strategy.pdf.

Transmetric. 2023. Transmetric. *Top 5 Benefits of Integrating AI in Logistics.* [Online] 05 11 2023. [Cited: 27 03 2025.] https://www.transmetrics.ai/blog/ai-in-logistics/.

U.S. Army. 2024. U.S. Army. *Army launches pilot to explore generative AI for acquisition activities.* [Online] U.S. Army, 18 October 2024. [Cited: 30 03 2025.] https://www.army.mil/article/280500/army_launches_pilot_to_explore_generative_ai_for_acquisition_activities.

Varpina, Zane. 2018. The Friedrich Ebert Stiftung Foundation, Baltic States. *Countries of old men? Demographic challenges in Estonia, Latvia and Lithuania.* [Online] 02 2018. [Cited: 05 02 2025.] https://baltic.fes.de/fileadmin/user_upload/documents/FES_Countries_of_old_men_final.pdf.

Verschuur, Jasper, Koks, Elco, Jim W Hall. 2022. Nature Communications. *Ports' criticality in international trade and global supply-chains.* [Online] Nature Communications, 27 07 2022. [Cited: 27 03 2025.] https://www.nature.com/articles/s41467-022-32070-0.

Woodgate, Jessica, Ajmeri, Nirav. 2024. Macro Ethics Principles for Responsible AI Systems:. *Macro Ethics Principles for Responsible AI Systems:.* [Online] University of Bristol, 10 09 2024. [Cited: 24 03 2025.] https://arxiv.org/pdf/2208.12616.

Worsham, Vanessa et al. 2024. Army University Press. *Army Medicine and Artificial Intelligence. Transforming the Future Battlefield.* [Online] Army University Press, 05 2024. [Cited: 31 03 2025.] https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/May-June-2024/MJ-24-Army-Medicine-AI/.

COL Māris Utināns. Mission command in the realm of Artificial Intelligence

1. Introduction

Contemporary military conflict and full-scale conventional war waged by Russia in Ukraine are characterized by a high level of uncertainty, diffused battlefields where the civilian domain is mixed with combatants, and legitimate military targets are integral parts of civilian shared infrastructure. Lethal weapon systems as military instruments of power cover all domains, expanding into the cyber and space domains. NATO visualizes the changing character of war through the Warfighting Capstone Concept (NWCC), where Warfighting turns out to be more multi-regional, multi-dimensional (physical, virtual, and cognitive), and expanding in a multi-domain operating environment (NATO_ACT, 2021). Besides the changes in the character of modern warfighting, the operational environment is evolving and brings new dilemmas to strategic decision-making. NATO, through NWCC, describes the operational environment as Persistent – increasing multiple actors (state and non-state) will compete for power and advantages. Simultaneous – rivals will use all means and instruments of power available at once, engage all accessible domains, and simultaneously be coercive from one perspective and cooperative from the other to achieve their desired end state. In addition to that, the operational environment becomes Boundless. That means that boundaries will blur not only between regions but also between military and political actions and even between physical and non-physical (cyber, information, etc.) domains (NATO_ACT, 2021). Another important driver of changes in contemporary warfighting is the rapid development of advanced military technology – quantum computing, artificial intelligence, and autonomous systems. At this point, we can conclude that decision-making at the strategic level will become more demanding and evolve to process an enormous amount of information. The decisions should be made based on trusted, multi-dimensionally coordinated, and timely relevant information. The recent development of machine learning (ML) and artificial intelligence's (AI) outraging capabilities makes AI/ML more extensively and broadly used in data analysis and decision-making. As the primary NATO command philosophy and decision-making principle, Mission Command faces a new realm of rapidly emerging Artificial Intelligence integration in decision-making at strategic and operational levels. Therefore, my research paper will focus on how AI influences mission command philosophy at the strategic level. The advantage of AI is the ability to autonomously process large amounts of data from unlimited databases, sensors, and systems. Based on processed information, AI can derive conclusions and aggregate options for decision-making.

To evaluate AI's influence on Mission Command and its interactions, the thesis of my research paper is as follows – even though AI-enhanced and autonomous systems have become more capable and require less human interaction in the execution of tasks, the primary role is still in the hands of commanders and decision-makers will applying the philosophy of Mission Command.

As described in the Army Doctrinal Publication ADP 6-0, one of Mission Command's core principles is that commanders practice principles to empower subordinate decision-making and decentralized execution appropriate to the situation (US_Army_HQ, 2019). On the other hand, while AI-enabled systems support commanders and decision-makers at strategic levels with the ability to have immediate situation awareness across multiple domains, it could lead to the desire to apply direct command philosophy and limit subordinate commanders' ability to make independent decisions.

At the beginning of my research paper, I will overview the main principles of mission command and how it is realized in NATO's strategic decision-making process. The following research objective elaborates on AI in military decision-making and how AI shapes Mission Command principles. Based on these findings, I will conclude whether the Mission Command philosophy is still relevant and what could be the essential requirements to ensure the effectiveness of military leaders in decision-making.

2. Mission Command at the NATO HQ strategic level.

At all levels, commanders' ability to gain initiative and establish favorable situations towards opponents is a prerequisite to victory. To accomplish that, it is essential to excel in decision-making to ensure the decision-making cycle is more efficient and effective than opponents. When assessing lessons learned from the Ukraine war, a decentralized and flexible C2 force arrangement is much more effective and resilient than a highly centralized hierarchical architecture (Berenguer, 2024 p. 4). To achieve this, NATO's main command philosophy is mission command, which ensures that the commanders exercise flexible, sound, and timely decisions. While Mission Command philosophy originated in German Auftrasgtaktik, in my research paper, I will use the ADP 6-0 publication to elaborate on the principles of mission command philosophy.
Mission command is the Army’s approach to command and control that empowers subordinate decision-making and decentralized execution appropriate to the situation. Mission command supports the Army’s operational concept of unified land operations and its emphasis on seizing, retaining, and exploiting the initiative (US_Army_HQ, 2019 Ipp. 1-3).

As it derives from the definition, the primary purpose of mission command is to seize, retain, and exploit the initiative. Significantly, when a centralized command structure is disrupted or lacking, or the situation within the battle space does not correspond to assumptions made before, the commander is encouraged to make sound decisions in compliance with higher commander-given intent. By that approach, subordinated commanders do not waste time by seeking guidance from higher echelons (as it is strictly required in direct command principles). Besides time, communication with higher command levels could not be possible because of disrupted communication and other limitations. Commanders' initiative in decision-making is critical not only on the battlefield but also in making sound decisions in everyday problem-solving when lacking directions and guidance from a higher command level. At the strategic level, where uncertainty and situation complexity prevail, and coordination with national Capitals is not possible, decisions should be taken solitary based on situation understanding and given authorization. To master Mission Command, the nations must constantly practice it. Principles of mission command should be followed in all domains of operation and on all command levels. When analyzing NATO strategic decision-making at the NATO HQ level depicted in Figure nbr.1, it is evident that mission command is the most effective command philosophy applicable to the NATO strategic level. Because decisions in the NATO HQ are based on consensus (32 member nations), all political (North Atlantic Council (NAC)) and military (Military Committee (MC)) considerations should be aligned.

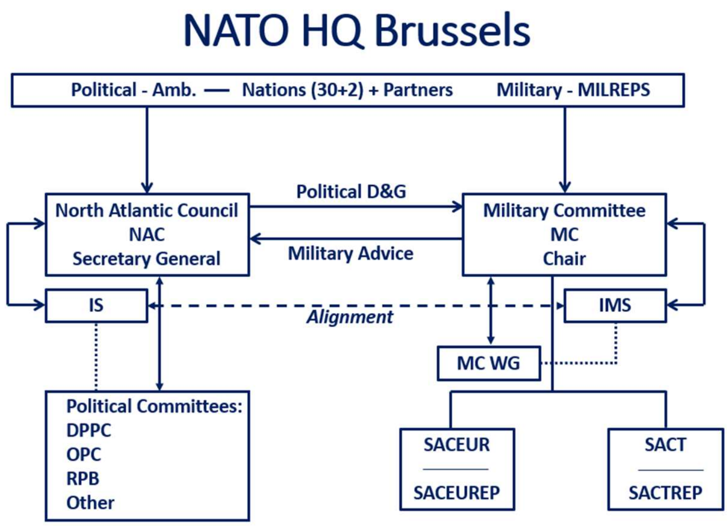

Figure 1. NATO HQ Brussels decision-making flow.
Source: (BALTDEFCOL, 2025)

Another factor in NATO's strategic decision-making is its complexity. Complexity is rooted in the scope of multi-domain operations, diverse political environments, and different nations' perceptions. To describe Mission Command's role at the strategic, I will refer to the main principles of Mission Command.

Mission command principles: (US_Army_HQ, 2019 pp. 1-7).

- Competence
- Mutual trust
- Shared understanding
- Commander’s intent
- Mission orders
- Disciplined initiative
- Risk acceptance

1.1. Competence.

Competence - Commanders and subordinates' ability to perform assigned tasks to the standard required (US_Army_HQ, 2019 pp. 1-7).

Competence is a significant prerequisite for commanders, subordinates, and higher political and military authorities to execute the command effectively. Competencies include multiple dimensions: professional competencies to be qualified in his expertise and assigned to respective committees and working groups. The following competencies strictly relate to the knowledge of NATO HQ functioning, decision-making process, and interactions between entities. The prerequisites for sustaining and building required competencies are the commander's and higher authority's commitment to the training and education of personnel. Training and education should include all contemporary challenges and uncertainties. The NATO Warfighting Capstone Concept (NATO_ACT, 2021) describes new battle space realms and challenges that require new competencies for military and political leaders. Competencies concerning emerging disruptive technologies include artificial intelligence-assisted systems, quantum computing systems, and autonomous systems. NATO's decision-making process and mission command principles should be part of education. Personnel will increase their knowledge and experience through regular comprehensive all-domain exercises and build self-confidence and trust in subordinates.

1.2. Mutual trust.

Mutual trust - shared confidence between commanders, subordinates, and partners that they can be relied on and are competent in performing their assigned tasks (US_Army_HQ, 2019 pp. 1-7).

Mutual trust is fundamental at a strategic level because when military leaders/political representatives are assigned to the NATO HQ, their primary purpose is to represent their nation's/Chief of defense or ministers. So, this mutual trust should be established before appointment at the NATO HQ. Mutual trust should be developed and practiced within national delegations and between other delegations and command levels. Trust is developed through shared values, education, training, and everyday interaction. So, if mutual trust is not established, then more direct control will be employed, and superior commanders/representatives will not delegate appropriate authorities. Therefore, it will cause a situation when a decision/action could be delayed. Building mutual trust is a long-lasting process that must be constantly practiced. Mutual trust is critical in fostering initiatives and self-development.

For example, common exercises and personal interactions are one way of building mutual trust, as described in ADP 6-0. A common background, education, understanding of doctrine, and a common language are required in strengthening mutual trust (US_Army_HQ, 2019 pp. 1-8). At this point, we can stress that the standardization of the education system and requirements in the NATO alliance enables a common understanding of doctrine and processes and reinforces shared values. Within NATO training and education, conducting multinational courses and exchanging students is a common practice, which facilitates building cultural awareness, sharing historical backgrounds, tightening personal relations, and establishing a solid foundation for mutual trust. Like one of the NATO professional military education establishments, the Baltic Defence College is a clear example – where multiple NATO and partner nations are obtaining knowledge based on NATO doctrine and common values. Professional military education establishments play an essential role in NATO, enabling the establishment of common doctrinal understanding and a platform for introducing new military technologies and practices from contemporary battlefields.

1.3. Shared Understanding.

A shared understanding – understanding of an operational environment, an operation's purpose, problems, and approaches to solving problems among all parties involved (US_Army_HQ, 2019 pp. 1-8).

The complexity of modern comprehensive multi-domain operational environments has become one of the primary challenges for command structure and the Mission Command philosophy in general. Comprehensive multi-domain operational space comprises more than traditional military domains; it includes non-military and cognitive domains. NATO's understanding of multi-domain operation (MDO) is that multi-domain operations refer to the push for NATO to orchestrate military activities across all operating domains and environments. These actions are synchronized with non-military activities and enable the Alliance to create desired outcomes at the right time and place (NATO_ACT, 2023). Consensus is the only principle to commence in all NATO operations and activities. Reaching a consensus is one of the elements of building a shared understanding between all 32 NATO nations. Multiple forums, working groups, and decision boards establish collaboration between political and military components. The main goal is to reach a common agreement on the situation across all domains and what is more critical to reach a consensus on the desired effect. The inclusive collaborative and comprehensive planning and decision-making process is required and practiced to achieve effectiveness. In case of deviation from shared understanding, consultation processes between the nations are used. Close coordination between the strategic commanders and higher political representatives fosters shared understanding. Commanders/representatives at all levels should demonstrate openness, be critical, and communicate their vision and intent. Besides formal forums, personal relations are important for establishing unofficial communication possibilities to reinforce the statements and introduce new ideas.

1.4. Commander's Intent.

The commander´s intent is the commander's clear and concise expression of what the force must do and the conditions the force must establish to accomplish the mission. It is a succinct, written description of the commander's visualization of the entire operation and what the commander wants to achieve (NSO, 2019 pp. 2-3).

At the strategic level, where NATO HQ defines political-military decisions where NATO 32 nations' positions should be determined based on consensus and driven by NATO core tasks (Deterrence and Defence/Crisis Prevention and Management/Cooperative Security) should be communicated and translated to NATO strategic Commands Allied Command Operations (ACO) and Allied Command Transformation (ACT). To achieve synergy in the effort, detailed and collaborative planning is practiced, during which strategic commanders, besides personal interactions, share their vision and military advice to the Military Committee (MC) and the MC to the North Atlantic Council. A clear understanding of intent enables commanders at all levels to adapt, make necessary adjustments, and use all assets effectively. Commander’s Intent should be communicated through all means, including informal meetings.

1.5. Mission order.

Mission orders are directives that emphasize to subordinates the results to be attained, not how they are to achieve them (US_Army_HQ, 2019 pp. 1-11).

At the NATO strategic level, that is the only way to succeed with task accomplishment because the situation changes are so rapid that no directive order will survive till the commencing of execution. Mission order application at the strategic level strengthens mission tasks with reasoning (purpose) and how particular effects complement accomplishing the intent. Commanders' initiative and decisiveness will be key to a favourable disposition towards an opponent despite all operational challenges. However, Mission orders do not exclude strict control measures and coordination requirements, especially when conducting cross-domain or joint operations.

Once, it was stated during a presentation at the Baltic Defence College lecture (Strategic planning), “Strategic level commander's main purpose is allocation of resources and prioritization of achievements of strategic objectives.” (BALTDEFCOL, 2025). Therefore, the strategic command's main responsibility remains to derive and orchestrate these resources toward prioritized objectives.

1.6. Disciplined Initiative.

Disciplined initiative refers to the duty individual subordinates have to exercise initiative within the constraints of the commander’s intent to achieve the desired end state (US_Army_HQ, 2019 pp. 1-12).

Multi-domain operations in contested environments will always be unpredictable and dynamic, and some extraordinary/unpredictable cross-domain effects could initiate these changes. For example, cyber-attacks have devastating effects on civilian critical infrastructure that jeopardize the commencing of decisive AIR or LAND operations. Disruption of vital communication networks could inflict strategic dilemmas on Space operations, etc. Therefore, commanders should be able to make decisions alone while higher command levels are inaccessible. Another prospect could be when operational situations provide opportunities that could lead to decisive results – commanders should be able to recognize it and exploit it. By practicing disciplined initiative, commanders are encouraged to take the responsibility to adjust operational plans while still operating in support of common intent. When a commander changes his plan, he should constantly assess how it aligns with higher echelon intent and what level of risk he, as a commander, accepts. The sustainability of strategic operation integrity should be one of the critical milestones to be evaluated before making changes.

For example, ADP 6-0 describes a few factors that commanders should consider while practicing disciplined initiative:

> "When exercising disciplined initiative, neither commanders nor subordinates are independent actors. Subordinates consider at least two factors when deciding when to exercise initiative:
>
> - Whether the benefits of the action outweigh the risk of desynchronizing the overall operation.
> - Whether the action will further fulfills the higher commander's intent" (US_Army_HQ, 2019 pp. 1-12).

1.7. Risk Acceptance.

Risk Acceptance - commanders' ability to balance the tension between protecting the force and accepting and managing risks that must be taken to accomplish their mission (US_Army_HQ, 2019 pp. 1-13).

At the strategic level, risk management is one of the mechanisms used to measure threats and develop a consensus-based decision. Risk management is based on strategic and operational assumptions, capability gaps, etc., and vetting it against strategic and operational goals and gains. This process becomes more and more complicated because warfighting domains evolve to be more inclusive, comprehensive, and multi-domain operational. The number of factors and the unknown are increasing expediently. A wide variety of artificial intelligence-assisted systems are engaged to improve the ability to process all factors and speed up the process.

Emerging quantum technologies and machine learning enable autonomous data processing systems, robotic platforms, sensors, drones, and space-oriented weapon systems to become the new reality of warfighting, thereby shaping the realm of decision-making. Risk Acceptance remains the commander's prerogative, where experience, knowledge, and a comprehensive understanding of the environment will dictate how the commander will lead the strategic operation and where he is ready to accept the estimated risk.

In this paragraph, we analyzed Mission Command and how Mission Command principles are incorporated into NATO HQ. In conclusion, we can see that the Mission Command philosophy, even in the light of contemporary comprehensive, multi-domain operational challenges, is still applicable and effective. Mission command will function only if introduced entirely in all aspects of principles. All NATO and partner nations should share principles of Mission command philosophy.

3. Artificial Intelligence influence on Mission Command.

The complexity of contemporary and future warfighting evolves widely beyond the regular joint operation framework. The weaponization of all instruments of power (not only the military) demands different approaches and tools for NATO to address security challenges. Multi-domain operations and cross-domain synchronization require more complicated mechanisms to obtain reliable situation awareness at all levels. Detailed all domains of intelligence information fusion build an enormous amount of information that ordinary human capabilities cannot process within the time required. Therefore, NATO's digital transformation and new emerging technologies incorporating artificial intelligence (AI), autonomous systems, and quantum computing could facilitate establishing and maintaining credible strategic situation awareness. Situation awareness is not only on opponents but also on friendly domains, and that situation awareness is to be shared among all levels of command. Everyday situation awareness will ensure shared understanding and strengthen the NATO alliance's effectiveness in fulfilling core tasks.

SUN TZU stated the importance of credible self-awareness and knowledge of the enemy as one of the criteria for success.

“If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained, you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle” (Sun Tzu, Cleary, Thomas Francis, 2005).

Effective communication and information exchange capabilities should support situation awareness as a prerequisite for effective command and control. All information should be blended comprehensively, and time for analysis should be as minimal as possible, reaching superiority over the opponent OODA (observe, orient, decide, and act) loop process. The information is generated across all domains and collected through numerous sources like sensors, computer networks, images, real-life streaming data, and unclassified and classified sources. This will cause a challenge for the decision-makers because the data will be overwhelming, contradicting, and generic. To process all technical information, artificial intelligence, and its assisted systems will conduct data analysis, provide decision-making advice, and suggest subsequent activities.

While implementing the machine learning principle, AI could monitor, compile, and compare previous data analysis, share results with complimenting sensors, define patterns, and make recommendations for the following data collection (Cook, 2021 p. 46). AI-assisted systems will support strategic command in establishing, maintaining, and sharing information, facilitating understanding of shared situations, reducing uncertainty, saving time, and speeding up the OOD loop process. At the strategic level, it is imperative to analyze situations from multiple perspectives, and understanding should be cross-domain, evaluated, and comprehensively coordinated. From the perspective of mission command, we see that AI supports commanders and decision-makers in maintaining uninterrupted shared understanding while reducing uncertainties and speeding up information dissemination between command levels.

The subsequent operational effect ensured by AI predictive analytics and driven by machine learning (ML) gives the possibility to model strategic situations and suggest responses, derive options and opportunities to predict future developments, and what critical responses are required. What is Predictive AI – Predictive artificial intelligence involves using statistical analysis and machine learning to identify patterns, anticipate behaviours, and forecast upcoming events (Mucci, 2024). With the complexity of multidomain operations, where strategic effects should be orchestrated across different domains, AI-assisted planning tools like the Joint All-Domain Warfighting Software (JAWS) program have become more helpful. Following systems strengthen military leaders' and decision-makers competence, and possible misjudgments are lower. That is possible because JAWS enables the strategic commanders to comprehend multiple operational domains and ensure seamless coordination of effects across all theatres of war. All technical judgments and calculations are based on the most accurate understanding of the situation, including friendly forces/actors and opponents' situation. JAWS supports strategic leadership in coordinating strategic effects while the forces and effectors are dispersed across all theatres of war. JAWS and similar AI-enabled systems demand credible and resilient network-centric and cloud-based capabilities, ensuring that all systems, sensors, effectors, and command nodes interact flawlessly. Additionally, an AI-assisted system will advise allocating the most appropriate capability in the most effective time and space (Keller, 2025).

While such a system enables commanders at higher levels to obtain timely information across all levels of command and domains, they could be willing to practice direct command principles. However, operational and strategic challenges will still require decentralized operational execution where trust, clear intent, and other Mission Command principles will ensure the operation's success.

Another example of AI/ML-assisted commander’s decision support is the Joint All-domain Command and Control System (JADC2). This project aims to improve commanders' informational awareness through real-time data availability and AI-supported predictive analysis through six product lines: sensor integration, data, secure processing, connectivity, applications, and effects integration (McGiffin, 2024 Ipp. 88). For strategic-level decision-makers, such systems will provide opportunities to comprehend strategic complexity considerably more easily, where technical data will be processed automatically, and reasoning will be the main component for decision-makers to assess. To interact effectively with JADC2 and similar systems, all level commanders should build trust in the system and trust between all command levels when knowing that AI/ML-assisted tools are used in the decision cycle.

Therefore, from a mission command philosophy standpoint – decision-makers should build trust in modern systems and develop competencies in how these systems contribute to modern warfare.

AI/ML-assisted decision support systems are a potential platform to incorporate autonomous systems, and introducing autonomous weapon systems creates a new realm of battle space that requires thorough ethical discussion. Discussion and decisions should be made about the human role in decision-making and the possibility of optimizing the "Kill Chain" process. What should the human role be in implementing an autonomous weapon system? Should it be a strictly man-machine decision/process (human make decision), or could humans be placed on the top of the decision cycle (human overwatch and is ready to intervene) or even excluded from it in some situations?

Besides executing warfighting functions, AI systems foster war gaming/simulation exercises where decision-making can be practiced in synthetic AI-generated reality. AI-generated reality will constantly evolve based on contemporary practice and situational developments in real-time events. We can conclude that AI/ML-assisted systems foster NATO strategic commanders' decision-making practice. Commanders at all levels and political leaders share the same situational understanding across all domains. Strategic effectors (weapon systems, platform, force, etc.) are much closer to the command level and could be coordinated across domains more effectively. Practical application of modern AI/ML-assisted systems should be the "new normal" at all command and decision-maker levels. During the exercises, strategic leaders would be able to understand the systems' capabilities; as it is an AI/ML-enabled system, machines would understand the strategic level's requirements and give more relevant outcomes for decision-making.

In conclusion, AI/ML-assisted decision and command systems (such as JAWS/JADC2, etc.) support the application of the Mission Command philosophy. Automating processes and autonomous systems reduces uncertainties and provides options for executing decisions and commands. AI supports sustainment and fostering shared understanding through the accessibility of the same situational understanding between command levels across all domains. Strategic commanders have more options to communicate their intent. Mission orders are prerequisites at a strategic level, where AI supports decentralized execution and initiative for subordinate commanders by ensuring cross-domain situation awareness and options to synchronize effects.

At the same time, AI/ML brings conceptual tensions and challenges that should be considered and assessed thoroughly (ethical dilemmas, human-machine interaction, the credibility of judgment, etc.). Modern battlespace requires a clear understanding of how and to what extent rising disruptive technologies, AI, autonomous systems, and quantum computing could be engaged in defense enterprises.

4. NATO's approach to AI in defense

Mission command based on competencies, mutual trust, shared understanding, commander's intent, mission order, disciplined initiative, and risk acceptance should treat AI as one of the members of the decision-making enablers. Therefore, a clear understanding of AI should be reached, understanding the system's capabilities, limitations, and reasonings; based on this knowledge, decision-makers at all levels could build trust in AI. Clear risk mitigation measurements should be established and followed when evaluating potential dilemmas and risks caused by AI. While exploring AI implementation in the military and not only military operations, the NATO alliance introduced principles for developing and implementing AI in defense. Ethical principles and the rule of law are fundamental, significantly when AI implications' full result and outcome are not comprehended while engagement in decision-making becomes more obvious and critical. NATO has agreed on six critical principles for addressing AI in defense: lawfulness, responsibility and accountability, explainability and traceability, reliability, governability, and bias mitigation.

- Lawfulness: AI applications will be developed and used in accordance with national and international law, including international humanitarian law and human rights law, as applicable (NATO_HQ, 2021).

Attribution to national and international laws is crucial, especially when war and armed conflicts enforce uncertainties, devastations, and atrocities. AI should not be designed without these regulations since we should understand that AI is not accountable, and humans should bear responsibility for AI actions and root causes.

- Responsibility and Accountability: AI applications will be developed and used with appropriate levels of judgment and care; clear human responsibility shall apply in order to ensure accountability (NATO_HQ, 2021).

AI becomes more autonomous, and human interaction becomes smaller. AI-assisted systems take the lead in data processing and are used in target acquisition and allocating more appropriate effectors. Based on a given task, AI solitary could deliver the effect on the target. Therefore, reaching a superiority over the enemy shortens the "Kill Chain." Applying clear rules will determine what exclusively should be human responsibility and what role and tasks for AI. Targeting is only one example where the rest of the ethical and moral dilemmas will evolve, for instance, Brain-computer interface technology application in the military to enhance human capabilities, etc. Based on tasks, humans still should have the option to break/control AI. AI should be perceived as a tool or weapon, not something that comprehends, judge, and makes decisions.

- Explainability and Traceability: AI applications will be appropriately understandable and transparent, including through the use of review methodologies, sources, and procedures. This includes verification, assessment, and validation mechanisms at either a NATO and/or national level (NATO_HQ, 2021).

To build trust in AI and understand the outcomes of AI-assisted systems, all processes should be traceable and understood by humans. To have that understanding, it is possible to ensure that AI-assisted systems give false results, which could lead to critical circumstances. A transparent process will minimize the "Black Box" phenomenon that forces decision-makers to rely on the unknown magic of the Black Box to make all decisions.

- Reliability: AI applications will have explicit, well-defined use cases. The safety, security, and robustness of such capabilities will be subject to testing and assurance within those use cases across their entire life cycle, including through established NATO and/or national certification procedures (NATO_HQ, 2021).

AI used in Defence systems should be stable and reliable, minimizing the possibility that AI-supported critical functions are corrupted and could cause operational failure. Different-level AI systems should be evaluated based on their purpose and tasks. In contrast, more critical tasks and purpose-enabled systems are tested and certified in demanding conditions and under rigorous procedures.

- Governability: AI applications will be developed and used according to their intended functions and will allow for appropriate human-machine interaction, the ability to detect and avoid unintended consequences, and the ability to take steps, such as disengagement or deactivation of systems when such systems demonstrate unintended behaviour (NATO_HQ, 2021).

Human control over the system is imperative because humans wage kinetic and destructive actions, and humans should be accountable for these actions. At the same time, AI is deciding based on situation understanding where machines cannot always interpret the situation correctly (ethical, moral dilemma, etc.). Based on that, humans should have taken part in decision-making – humans in the process (humans make decisions to act on effect) and humans over the process (humans are an overarching process and ready to intervene).

- Bias Mitigation: Proactive steps will be taken to minimise any unintended bias in the development and use of AI applications and in data sets (NATO_HQ, 2021).

As an emerging new technology, AI should be fostered to be understood at all levels of command, especially at the strategic level. The decision-making should be literate on principles of how AI works and their possibilities and limitations. New command and decision-making procedures and systems should be introduced and trained daily. Based on these principles, AI will be more transparent and contribute to decision-making more constructively. At the same time, AI shapes modern battle space where interaction between humans and machines becomes more interconnected and interdependent – the principle of acceptable risk is still actual. It even demands to be applied to AI/ML-assisted systems, where all level commanders and decision-makers should evaluate and be able to take prudent risks when using AI/ML-assisted systems.

5. Conclusion

The evolution of Artificial Intelligence, autonomous systems, and quantum computing technologies have changed contemporary battle space and requirements to cope with all that complexity and diversity. Integrating AI and emerging disruptive technologies in military affairs is inevitable and crucial to reaching superiority in orchestrating complex cross-domain operations and exercising command in all theatres of war.

Even though AI and autonomous systems have become more capable and require less human interaction in executing tasks, the primary role in decision-making remains the commanders' and strategic decision-makers' ultimate responsibility. AI/ML-assisted systems complement the application of the Mission Command philosophy at the NATO strategic level, fostering mission command principles and ensuring the effectiveness of weapon systems across all domains.

Mission Command as a primary NATO command philosophy remains focal. Joint multi-domain operations require decentralized execution while synchronizing at multiple levels and across all operational domains is needed. Mission command enables all level commanders to build mutual trust, ensure shared situation understanding, adjust operations concerning the situation, and take the initiative when the strategic opportunity is present. At the same time, AI and autonomous systems support commanders in the fulfillment of the principles of Mission Command, reducing uncertainty, maintaining critical situation awareness, coordinating operational effects, and assessing numerous aspects and data. A comprehensive approach is the key to success at the NATO strategic level, and Mission Command principles endorse consensus-based decisions.

Principles of Mission Command are applicable even in programming AI and autonomous systems, especially in the context of acting without intervention from the human side. AI and autonomous systems bring ethical and moral dilemmas, which should be addressed constantly because the development of AI is just at its arising. The application of AI presents wicked challenges while increasing human capabilities (for example, brain-computer interface (BCI), general AI, etc.).

6. Recommendations

Mission Command should be practiced at all command levels across all domains. All principles of Mission Command should be followed because if you miss one of them (for example, Mutual Trust, etc.), the decision-making and OODA loop will be seriously hampered. AI systems should be integrated into daily routines and should assist decision-making. Frequent comprehensive multi-domain exercises should be conducted, where AI should be challenged in an operational environment. Mission command principles should be focal when designing exercise and execution, therefore practicing it and experimenting with outcomes. Predictive AI should be used when new concepts and strategic decisions are exercised, thereby simulating scenarios that are as real as possible.

To ensure effective decision-making in collaboration with AI. Adapting the Professional Military education system and Civil leadership training regarding AI, autonomous systems, quantum computing, and other disruptive technologies is critical in understanding technologies' capabilities, limitations, and application possibilities. Building trust in AI and understanding its limitations will ensure effective integration and collaboration between humans and machines. Mission Command principles will help the integration of AI/ML at the strategic level.

The evolution of AI should be closely monitored and assessed. Clear strategies and guidelines should be established to ensure that moral and ethical considerations are evaluated and implemented. This process should be continuous because the development of AI and its application is and will progress in different forms and volumes.

Mission Command philosophy should be reinforced by modern technologies, even attributed to the new military technologies. Strategic commanders and leaders should be equally educated and trained when modern technologies are inaccessible or disrupted so the Mission Command philosophy prevails.

Robust information and communication systems should reinforce Joint All Domain Command and Control systems. Existing NATO alliance command structures could be revised and reassessed while Mission Command principles remain focal.

Bibliography

BALTDEFCOL. 2025. *NATO HQ Decision Making Processes.* Tartu : Presentation , 2025.

Berenguer, Victoriano Vicente Botella. 2024. FINABEL. *The European Land Force Commanders Organisation.* [Online] 23 October 2024. [Cited: 18 March 2025.] https://finabel.org/wp-content/uploads/2024/10/IF-PDFs.pdfxx_.pdf.

Cook, Brendan. 2021. *The Future of Artificial Intelligence.* s.l. : Air & Space Power Journal, 2021.

Keller, John. 2025. Military+Aerospace Electronic. *Home stretch eyed in project to develop large-scale military planning software with predictive analytics.* [Online] 22 January 2025. [Cited: 23 March 2025.] https://www.militaryaerospace.com/computers/article/55262215/military-planning-software-using-predictive-analytics.

Manzi, Graeme. 2024. Karve . *Revolutionising Defence Intelligence, Surveillance & Reconnaissance (ISR) with AI.* [Online] 13 February 2024. [Cited: 23 March 2025.] https://www.karveinternational.com/insights/revolutionising-defence-intelligence-surveillance-reconnaissance-isr-with-ai.

McGiffin, Joseph M. 2024. Mission (Command) Complete Implications of JADC2. *Joint Force Quarterly.* 2024, Vol. 113, 1/14.

Mucci, Tim. 2024. What is predictive AI? *IBM.* [Online] IBM, 12 August 2024. [Cited: 24 March 2025.] https://www.ibm.com/think/topics/predictive-ai.

NATO_ACT, NATO's Strategic Warfare Development Command. 2021. Allied Command Transformation. *NATO Warfighting Capstone Concept.* [Online] 2021. [Cited: 03 March 2025.] https://www.act.nato.int/our-work/nato-warfighting-capstone-concept/.

—. 2023. Multi-Domain Operations in NATO – Explained. *ALLIED COMMAND TRANSFORMATION.* [Online] NATO, 5 October 2023. [Cited: 21 March 2025.] https://www.act.nato.int/article/mdo-in-nato-explained/.

NATO_HQ. 2021. North Atlantic Treaty Organization. *Strategy for Artificial Intelligence.* [Online] NATO HQ Brussels, 21 October 2021. [Cited: 01 April 2025.] https://www.nato.int/cps/en/natohq/official_texts_187617.htm.

NSO, NATO Standartization office. 2019. Allied Joint Doctrine for The Planning of Operation. *NATO ACT.* [Online] 24 May 2019. [Cited: 21 March 2025.] https://www.coemed.org/files/stanags/01_AJP/AJP-5_EDA_V2_E_2526.pdf.

Seeds, Michael. 2024. Pentagon Sorting Out AI's Future in Warfare. *National Defense Magazine.* [Online] National Defense Industrial Association, 22 10 2024. [Cited: 13 02 2025.] https://www.nationaldefensemagazine.org/articles/2024/10/22/pentagon-sorting-out-ais-future-in-warfare.

Sun Tzu, Cleary, Thomas Francis. 2005. *The Art of War.* s.l. : Harper Press, 2005. B004TVXZ3K.

US_Army_HQ. 2019. *ADP6-0 Army Doctrine Publication.* Washington D.C. : Army Publishing Directorate, 2019.

BEST ESSAY OF THE COMMAND SENIOR ENLISTED LEADER'S COURSE (CSELC).

CWO Wayne Bantock. “Feline Rivalry” A Comparison Between Leopard 1 and Leopard 2 in Ukraine

The war in Ukraine has fostered much discussion and debate regarding the employment of various combat systems. There has been a myriad of systems procured and donated to Ukraine, some of which are quite old and considered obsolete.

Ukraine is dealing with a logistical nightmare. They are using multiple types of equipment designed for the same task, most of which have little or no interchangeability with regards to ammunition parts and training.

This paper will focus on a comparison between the Leopard 1 and Leopard 2 main battle tanks to determine which is the right tank for Ukraine (The Shephard News Team. 2023).

There are many factors to discuss when debating the effectiveness of an armoured vehicle. In this paper, I will not only focus on firepower, mobility, and protection but will also look at multiple, often overlooked aspects of comparison, such as sustainability and cost.

The reader will undoubtedly concur that the Leopard 1, though older, is an ideal fit, right now, for the Ukrainian Army (Kyiv Post. 2023). To prove this, I will leverage multiple references, personal interviews and my own experience working with these platforms domestically as well as while deployed in Afghanistan.

Historical Context

It is important to understand the background and rationale behind the development of these related but completely different tanks.

The Leopard 1 was designed in the 1950s but implemented in the 1960s. It was Germany's first post-war tank. It was designed to fight a kinetic full-scale conflict in Europe. Its design emphasised speed, mobility and flexibility of employment. Consequently, it sacrificed heavy armour as this was felt, at the time, to be a risk worth accepting. Many NATO armies adopted it and many variants were built, including recovery, bridge layer, anti-aircraft etc (National Interest. 2022).

The Leopard 2 was developed in the 1970s and outfitted with a heavier main gun and much more armoured protection. Though an excellent platform these attributes came with a price. This much heavier tank was larger and far more complex which led to sustainment and mobility challenges that were easily overcome by nations with adequate resources but challenged others with smaller budgets (National Interest. 2024).

Firepower

The Leopard 2 is equipped with the proven and very capable Rheinmetall 120 mm smoothbore. It is very accurate, has excellent fire control systems and is more than capable of dealing with any potential adversaries in the field in Ukraine at long range. The fire control systems on the Leopard 2 are excellent, but very complex to repair, especially in field conditions (Popular Mechanics. 2024).

The Leopard 1 is equipped with the Royal Ordnance 105mm L7 rifled gun, although effective it does not compete with the Leopard 2 in terms of overall firepower. It does however have the ability to destroy most of the soviet era tanks that it may encounter in Ukraine. It also is much easier to maintain due to its relative simplicity. There is also a significant amount of the cheaper 105 ammunition available including the high explosive and high explosive squash head (only suitable for use in rifled barrels) variety which is excellent for infantry support operations and indirect fire. Ukraine views the indirect fire role as a highly desirable capability. BGen Steve Graham, a senior Canadian Armoured Officer told me about the Leopard 1 Gun Laying Instrument which was a device mounted on the side of the breach. This enabled the crew to adjust fire in the indirect role. This capability was practised routinely with the Leopard 1 but is not a regular part of training with the newer tank.

The availability of 105 mm tank ammo is great because many NATO countries no longer use it as most are now using the 120 mm type. This means that some NATO countries may have large stocks of 105 mm ammunition that they can donate. (Wikipedia. 2024).
The versatility of the older gun and its less complex fire control system cannot be overstated, it has enabled the Leopard 1 to be employed in many different roles and has multiple backup systems that keep the system serviceable.

A senior retired NATO Officer working in Ukraine told me that, "so far there have been very few actual tank vs. tank actions in the war so the advantage that the Leopard 2 holds in terms of firepower has not been exploited. The diversity of the Leo 1 ammunition and versatility of employment is therefore actually advantageous".

Mobility

This is another especially important characteristic when referring to armoured vehicles. When we compare the two platforms the Leopard 1 is much lighter at 40 tons compared to the Leopard 2 at approximately sixty-two tons (Forces News. 2023).

The advantages to this are multiple. The terrain in Ukraine is varied, there is rough, uneven ground, wetlands, numerous wet gap crossings as well as urban environments. The lighter tank can move swiftly and exploit tactical advantages quickly as well as conceal itself easily due to its lower profile. This is especially advantageous in urban combat. The nimble Leopard 1 can navigate built-up areas and can use its high explosive squash head rounds to great effect to dislodge enemy troops in buildings or fortifications. Its smaller overall size can negotiate damaged urban environments and make it an ideal platform for fighting with infantry in built-up areas (Forces News. 2023). The Leopard 1's lighter weight also allows it to traverse bridges that the heavier Leopard 2 cannot. This means the Leopard 2 must use engineer assets like pontoon bridges or rafts. The lighter Leopard 1 is ideally suited for fighting short, sharp, hit-and-run style engagements, especially in areas where the Russians may have superior firepower.

The Leopard 2 can cross wet gaps as deep as 4 meters but there is a significant amount of preparation involved (Euro SD. 2024). This can make crews and vehicles vulnerable to enemy detection and subsequent fires. The Leopard 1's ability to use most civilian-built bridges allows it to cross quickly without lengthy preparation or valuable engineer assets.

Modifications to improve the Leopard 1 are available. For example, Rolls Royce has created an upgrade to the power pack which would increase the horsepower of the tank dramatically from an output of 190 kW to approx. 800kW. This is a significant improvement which will enhance the tanks speed and mobility, and no doubt improve reliability and serviceability rates (Army Recognition. 2024).

The fact that the older tank is lighter also means that it can be transported more easily using trains or trucks. This is important when moving vehicles forward into the fight or when backloading them for repairs. When Leopard 2 becomes stuck or breaks down it requires the Leo 2 Armoured Recovery Vehicle. This vehicle or similar variants like the M-88 are the only armoured recovery vehicles capable of recovering it. As such it is in high demand and a high-value target for the enemy. Getting a tank to the front line quickly is critical, the lighter weight of the Leopard 1 can facilitate quicker response times and greater flexibility in the varied terrains prevalent in Ukraine.

Protection

The Leopard 2 has very thick composite armour, (Army Recognition. 2022) which makes it far more resistant to enemy fire. The Leopard 1 conversely has thinner steel armour which, at the time of its introduction was done intentionally to enable it to move quickly on the battlefield. The employment of Leopard 1 in an indirect fire role also reduces the risk to the crew as it can engage the enemy from concealed positions. There have also been modifications to the Leopard 1 to increase its armoured protection, the Canadian MEXAS kit is a great example, but this added weight hinders the mobility of the tank. Anti-drone nets have also been added to many platforms in Ukraine. The net is designed to catch the drone and mitigate the explosive charge through standoff protection. The Ukrainian Army has also added explosive reactive armour as well as anti-drone nets to Leopard 1 to improve its survivability (Kyiv Post. 2024).

Heavily armoured tanks are being destroyed on the battlefield by lightweight, handheld anti-armour weapons as well as drones such as the Russian Lancet. Therefore, the Leopards 1's lightweight and lower profile gives it an advantage as it is a more difficult target to identify and target by enemy anti-armour teams. The higher crew survivability factor in the Leopard 2 cannot be ignored. But the agility, mobility and modifications to improve the survivability of the older tank as well as employing it in hit-and-run, ambush-style tactics and not in head-on engagements helps to mitigate its reduced armour protection.

Accurate numbers of Leopard 1 and Leopard 2 tanks destroyed are very difficult to find. Obviously, both sides of the conflict want to keep losses as close hold as possible. However, it is obvious that both tanks have strengths and weaknesses that must be recognised and leveraged in order to enhance crew survivability.

Sustainability

The ability to maintain, sustain and equip a combat system in battle is often overlooked. The previous factors of mobility, firepower and protection are often the only aspects that are discussed regarding armoured vehicles. A platform can have the best of all three of these vitals but is useless if it cannot be repaired, refuelled and re-equipped on the battlefield as far forward as possible.

The Leopard 2 is a very capable modern platform with complex state-of-the-art fire control systems and a power pack that is more powerful than the Leopard 1. Maintaining it is complex and requires skilled highly trained technicians using specialty tooling and equipment. This is ideal when a nation has the time and space to train technicians. Many Western nations provided technician training to Ukrainian soldiers, but this took them away from the fight for a significant amount of time and even then, they received a fraction of the training that NATO technicians receive. I have seen this first hand when visiting the Leopard Training Centre of Excellence in Poland.

BGen Scott McKenzie, a senior Canadian deeply involved in the Leopard transfer to Ukraine mentioned, "training on the Leopard 1 can be accomplished faster as the tank is less complex and easier to work on. This means the Leopard 1 is easier to keep serviceable with less speciality training for technicians".

The motivation of the Ukrainian soldiers is admirable but the training they are receiving on the Leopard 2 is bare minimum at best.

Complex systems can require more time to repair, I know this from personal experience. This is not ideal as the principal tenet of any army maintenance organization is to repair as far forward as possible, in the least amount of time to get a vehicle back in the fight quickly. Repairing close to the front is critical as supply lines are often disrupted during combat operations. Equipment is also very vulnerable when being towed or transported to areas far to the rear. Major repair and overhaul tasks on Leopard 2 must be performed in a secure area with the requisite infrastructure. This often means that complex equipment like Leopard 2 is backloaded to manufacturer facilities which can be located outside of Ukraine. This adds more time to the process and ties up heavy trucks which could be used for other sustainment tasks. Most repairs on Leopard 1 however can be done much closer to the front in first-line maintenance organizations. Major repairs will of course need to be backloaded, but this applies to all types of vehicles and equipment.

Parts availability is also a factor (Slashgear. 2024). The Leopard 1 has been in use for many years longer than the Leopard 2. Countries such as Greece and Turkey have significant stockpiles of parts and complete platforms that they may be willing to donate. Often, a country with both Leopard variants will donate the Leopard 1 with accompanying spare parts and ammo rather than their more modern Leopard 2 variants.

The disparity in fuel consumption between Leopard 1 and Leopard 2 is enormous. I saw this first hand as an RSM of a Combat Service Support Battalion. A Leopard 1 can operate much longer on a tank of fuel than the Leopard 2. This means that the logistics of refuelling are much more difficult and complex for the Leopard 2. It requires more fuel, more often and therefore more refuelling trucks and soldiers to operate them. More fuel trucks travelling on contested supply routes are very vulnerable to enemy fires.

The Leopard 1 has a smaller logistics footprint and is easier overall to maintain (Slashgear. 2024). This is a massive factor when resources are at a premium and lines of sustainment are jeopardised. Anything that has a lighter load to an already stressed sustainment system is very beneficial. The logistics chain in Ukraine is very complicated at this time. Multiple weapons systems and variants of the same platform as well as many different natures of ammunition make sustainment extremely challenging. Anything that can be done to simplify logistics is greatly appreciated. The simplicity of logistics and training is a war-winning factor that cannot be overlooked. This is a massive bonus when operating the Leopard 1 (Slashgear. 2024).

Cost

This is always a major consideration for countries, especially when they are at war. Economies are strained to the limit so any opportunity to save money by procuring effective weapons systems is crucial. Although many systems have been donated there is still a significant amount which has been purchased. Much of the equipment that was donated was lent to Ukraine, much like the lend-lease program during World War 2. It is therefore advantageous to get as much equipment as possible for the money. In fact more than 270 Leopard 1 platforms of all variants have been donated as opposed to 140 Leopard 2 variants. Size and weight become a factor when shipping large equipment. More savings in room and weight add up quickly when shipping large numbers of heavy armoured vehicles long distances. The difference in overall cost will allow Ukraine to employ more tanks for the same cost increasing the size and capabilities of its armoured force. This is yet another war-winning, but often overlooked, factor.

SWOT Analysis

Leopard 1 Strengths

1. Simplicity of Sustainment
    a. The Leopard 1 is easier to maintain and repair in the field, this keeps it serviceable longer, keeping it in the fight.
    b. Training time for crews and maintenance is much faster.
2. Weight, Size and Mobility
    a. The Leopard 1 is much lighter than Leopard 2 which means it has more mobility over rough terrain, has fewer restrictions with regards to bridge classifications and is ideal for urban combat in narrow streets.
3. Cost Effective

a. The Leopard 1 burns less fuel, is less expensive than Leopard 2 and is cheaper to operate in general than Leopard 2.
b. Lower cost allows for procurement of more platforms.

Leopard 1 Weaknesses

1. Armour Protection
    a. Leopard 1 armour is much lighter than the Leopard 2 which makes it vulnerable to enemy fires.
2. Older Technology
    a. The Leopard 1 uses older fire control and targeting systems than the Leopard 2.

Leopard 1 Opportunities

1. Versatility
    a. Can be used in more types of terrain due to its lighter weight.
    b. Ideal for hit-and-run tactics prevalent in Ukraine.
    c. Ability to be used effectively in the indirect fire role.
2. Modifications
    a. The Leopard can be modified to enhance protection from drones and anti-armour weapons.

Leopard 1 Threats

1. Enemy Tank Modernization
    a. If the enemy modernizes their tanks the Leopard 1 could be left behind technology-wise. This would enhance and expose Leopard 1 weaknesses and vulnerabilities.

Leopard 2 Strengths

1. Advanced Technology
    a. The Leopard 2 uses advanced fire control systems and modern armour providing excellent protection and overall survivability.
2. Firepower
    a. The 120mm smoothbore gun is cutting edge and is more than a match for any threat on the Ukrainian battlefield.

Leopard 2 Weaknesses

1. Cost
    a. The high price to procure and maintain can be a challenge. This is especially the case when countries are fighting an expensive protracted conflict as is the case in Ukraine.
2. Sustainment
    a. Its complex systems require significant training and maintenance support.
    b. Battlefield resupply with fuel and ammunition requires a large combat service support footprint.

3. Mobility
    a. Its heavy weight restricts its movement and versatility on the battlefield.

Leopard 2 Opportunities

1. The Leopard 2 is in use by many countries and support is still available from the manufacturer. This ensures that Leopard 2 used by Ukraine can be kept up to date and modified for emerging threats.

Leopard 2 Threats

1. Advancements in Warfare
    a. Rapid adaptation by the enemy developing weapons to negate the Leopard 2's strengths.
2. Donor Fatigue
    a. Contributing nations will likely reach a point where they can no longer afford to donate any more of their more modern platforms.

Conclusion

The Leopard 1 and 2 are both very capable platforms. When comparing these two tanks one can quickly conclude that the newer, more high-tech tank would be the better. This would be the case if the fighting in Ukraine was classic kinetic tank vs tank warfare. The fighting in Ukraine has seen extraordinarily little armoured clashes reminiscent of World War 2 battles such as Kursk or El Alamein.

The fighting in Ukraine is more often short sharp infantry support clashes with a hit-and-run focus. This type of warfare is ideal for the lighter nimbler Leopard 1. Its firepower is adequate for this type of combat and its high level of mobility is enhanced by its lighter weight. This means that it can utilize most bridges instead of relying on valuable engineering assets like rafts or bridges. The newer tank provides significantly more protection than the Leopard 1, this however is mitigated by the tactics in which it is employed. The Leopard 1 will not do well in a standoff fight with a modern Russian T-80, it can however hold its own when fighting from ambush positions.

The often-overlooked factors of sustainability and cost weigh heavily in favour of the Leopard 1. The older tank is far easier to maintain and keep in the fight. The fact that the Ukrainians can procure several Leopard 1 for the cost of one of the newer tanks is favourable. Training soldiers to fight and maintain the Leopard 1 is much faster than the newer more high-tech Leopard 2. This means that crews and technicians spend less time at schools and more time using the tank in combat (Forbes. 2023).

Leopard 1 is an ideal platform due to its simplicity of sustainment and training, low cost as well as the current nature of combat in Ukraine. Ukraine needs to simplify its processes and focus its efforts on larger fleets of simple to sustain effective fighting platforms.

Both platforms are excellent and have prevailed in the test of time. But like any other system, they need to be employed at the right time in the right place. The Leopard 1 is the right tank, right now for Ukraine.

Bibliography*

Italic note: *This bibliography does not fully comply with the course expectations, by providing titles of journalistic articles instead of the required name-date format.*

Larson, Caleb. 2022. After Decades, Germany's Leopard I Tank is Still Fighting Everywhere. *National interest* [Online] 27 Jan. 2022. https://nationalinterest.org/blog/reboot/after-decades-germanys-leopard-i-tank-still-fighting-everywhere-199897.

"Barely Recognizable – Ukraine Unveils its Upgraded Leopard 1 Tanks." 17 Sept. 2024, https://www.kyivpost.com/post/39110.

"Gap crossing: the challenges of water obstacles in Europe." 05 Mar. 2024, https://euro-sd.com/2024/03/articles/36873/gap-crossing-the-challenges-of-water-obstacles-in-europe/.

German Leopard 2A7V tank offers the best protection in the world." https://www.armyrecognition.com/focus-analysis-conflicts/army/defence-security-industry-technology/german-leopard-2a7v-tank-offers-the-best-protection-in-the-world

"How the Leopard 2 Tank Keeps Getting Better (As in More Lethal)." 09 Jan. 2024, https://nationalinterest.org/blog/buzz/how-leopard-2-tank-keeps-getting-better-more-lethal-208473.

"Leopard 1 v Leopard 2: How do the tanks bound for Ukraine compare?." 13 Feb. 2023, https://www.forcesnews.com/ukraine/leopard-1-v-leopard-2-how-do-tanks-bound-ukraine-compare

"Norway details Leopard 2 donation to Ukraine | Shephard." 14 Feb. 2023, https://www.shephardmedia.com/news/landwarfareintl/norway-donating-tank-package-to-ukraine/..

"Rolls-Royce and FFG upgrade Leopard 1 Main Battle Tank and Wisent 1 ...." https://www.armyrecognition.com/news/army-news/army-news-2024/rolls-royce-and-ffg-upgrade-leopard-1-main-battle-tank-and-wisent-1-mine-clearing-vehicle-with-advanced-mtu-8v199-engine

"Royal Ordnance L7 - Wikipedia." https://en.wikipedia.org/wiki/Royal_Ordnance_L7.

"The Biggest Differences Between Leopard 1 & 2 Battle Tanks." 12 May. 2024, https://www.slashgear.com/1578273/differences-between-leopard-1-and-2-battle-tanks/

"They May Be Old but They Can Still Outshoot the Russians - Leopard 1 Tanks." 15 Apr. 2023, https://www.kyivpost.com/post/15808

"Ukraine Is Getting A Lot Of German-Made Leopard 1 Tanks. That Means A ...." 19 Aug. 2023, https://www.forbes.com/sites/davidaxe/2023/08/18/ukraine-is-getting-a-lot-of-german-made-leopard-1-tanks-that-means-a-lot-of-training-for-ukrainian-tankers/

"Why the Leopard 2 Is Such a Badass Tank - Popular Mechanics." 16 Jan. 2024, https://www.popularmechanics.com/military/weapons/a41713287/why-the-leopard-2-is-a-badass-tank/..

BALTIC DEFENCE COLLEGE