AD SECURITATEM

THE BEST ESSAYS BY COURSE PARTICIPANTS AT THE BALTIC DEFENCE COLLEGE

ACADEMIC YEAR 2022/2023

BALTIC DEFENCE COLLEGE

TABLE OF CONTENTS

BEST ESSAYS OF THE JOINT COMMAND AND GENERAL STAFF COURSE

MAJ Tomas BALTRUNAS. What is the future of Special warfare? Is the current Joint Allied Special operations doctrine still valid or has to be adapted to contemporary military conflicts?

. “SOF must continue its current mission while adapting to great power conflict on new and unexpected battlefields.”

Taft et al., 2019

Introduction

After the Kremlin started the war in Ukraine, creating a security disbalance in Europe (Counter-Currents, 2022), Heads of State and Governments of the NATO Allied nations during the NATO Summit in June 2022 in Madrid adopted a new NATO Strategic Concept (NSC), the first time in Alliance history, clearly identifying Russian Federation as the direct danger to security, peace, and stability of NATO member states. Moreover, it emphasizes that the Euro-Atlantic area is no longer peaceful, and countries face a real threat to sovereignty and territorial integrity (NATO, 2022). A switch in understanding the threat coextensively led to a change in NATO’s primary purpose, going from Crisis Prevention and Management to Assurance of the Collective Defense of its members based on a 360-degree approach (NATO, 2022). Consequently, all the military components must make their recalculations changing their focus to the vis-à-vis fight against peer state competitors to remain effective on the contemporary battlefield. Special Operations Forces (SOF) are not an exception.

During the last few years, the special operations community, military leaders, and experts have widely discussed and analyzed SOF's role and transformation requirements. However, after the Russian Federation invaded Ukraine, the topic requires additional analysis; first, answering whether the current doctrine is still valid and effective for the nature of the current state-on-state military conflict.

Thus, this paper aims to argue that SOF remains a valuable and effective JF Commanders’ tool to achieve operational objectives and confirm that SOF principal

tasks defined by NATO Allied Joint Publication - 3.5 (AJP-3.5) Allied Joint Doctrine for Special Operations remain actual but must be revised and adapted to current threats and requirements of the contemporary battlefield.

The research is done from the lens of a smaller country. There is much controversy about whether quantitative or qualitative criteria are best suitable for characterizing the tiny state (Maass, 2009). Nevertheless, quantitative limitations and the actuality of the force preservation while the opponent has enormous numerical and firepower advantages are considered the most, analyzing what tools a small nation could use to resist an occupier and eventually win a war by not losing it (Pettersson, 2022). This paper defines a small state as a state with up to ten million population, and the size of the nation's SOF is under one thousand personnel.

The analysis recommends implementing changes to maintain effectiveness while conducting Special Reconnaissance (SR), Military Assistance (MA), and Direct Action (DA) operations (Figure 1. Research Construct).

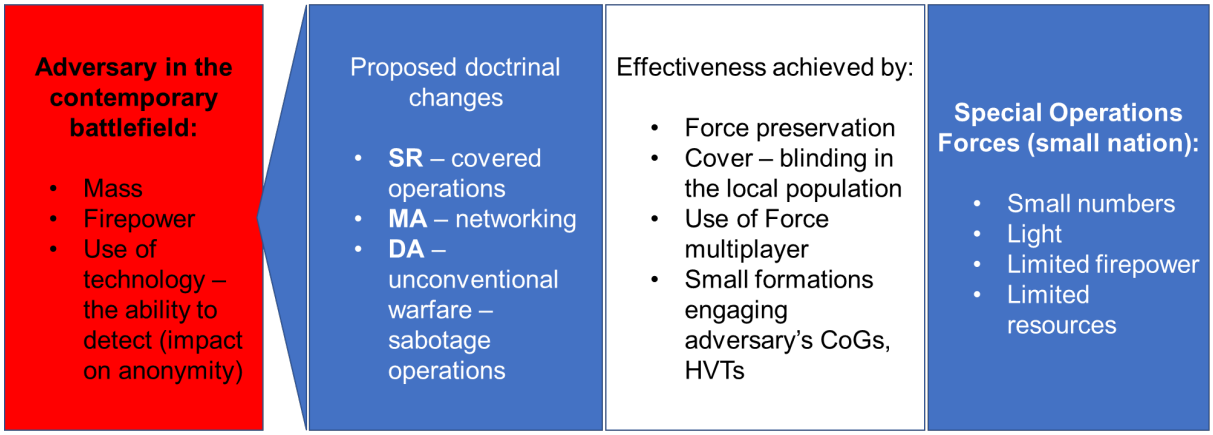


Figure 1. Research Construct

The first chapter of the paper provides the historical background and origins of the SOF, defines NATO Special Operations (SO), and answers the question of how SOF differs from conventional forces. The effectiveness of SOF executing its principal tasks in state-on-state fighting is analyzed in this paper's second chapter through the examples of its employment during World War II and the successful cases of the Ukrainian SOF operations against the Russian Armed Forces. The third, fourth, and

fifth chapters provide options for potential doctrinal changes to effectively cope with modern threats on the contemporary battlefield. The paper aims to expand the scholarly dialogue and provide strategists and military planners, including military decision-makers, with analysis-based recommendations for adaptation and potential implementation of changes in NATO SOF doctrine.

Chapter 1. The nature and fundamental tasks of the Special Operations

1.1. Back to the origins

The existence of specially trained troops - elite warriors, and unique purpose formations designed to accomplish missions could be obtained in sources from antique to modern times. Here are a few examples to illustrate the statement; the Crusades, units of Templars assaulting smaller Muslim groupings to capture prey; the elite warriors known as ninjas, trained across feudal Japan, equipped with the latest cutting-edge weaponry, and taught in martial arts, unique tactics, asymmetric warfare, and guerrilla fighting. Moving closer to modern times, Colonel Bassi of the Italian Army established a battalion-size task force named Arditi during WWI. The formation served as tactical impact sections, including wreaking havoc on the opposing side's fortifications and supporting infantry to advance further (Sof, 2022). Modern Western special operations organizations trace their origins primarily to WWII-era formations. Winston Churchill was an ardent supporter of special operations, hoping they would "light Europe ablaze" by executing massive raids and establishing resistance troops behind enemy lines (Titulaer, 2021). Finally, in later periods, SF was routinely utilized in military campaigns such as the Falklands War, Northern Ireland, Gulf Wars, Afghanistan, Kosovo, and Bosnia, and the siege of the Iranian Embassy in London. The above are just a few cases where special operators have participated over the years (Sof, 2022).

Given examples reflect that the specially trained and equipped soldiers, in most cases, significantly contributed to the success of the overall battle or campaign or been used for a specific task or to achieve critical objectives. Even in eras very far in the past, commanders have understood that it is beneficial to have a select set of warriors among their ranks who can do what others cannot (Sof, 2022). It is not only about the

construct of capture–kill operations; it also includes reconnaissance operations, which provide additional essential military intelligence components (Sof, 2022). Furthermore, operations to prepare and influence indigenous people to achieve desired effects, what nowadays is called Military Assistance. If to look carefully, all the given examples of the assigned tasks to the mentioned elite formations from the beginning have always been very close to what we have today, echoing the principal tasks of SO described by AJP-3.5 – SR, MA, DA. All of them will be defined in the following chapters of this research.

1.2. Special operations defined by AJP-3.5

The SOF truths state that “humans are more important than hardware” and “quality is better than quantity.” That said, the human factor contributes to Special Operations the most. It is a common rule that standards of selection and training of SOF personnel are the responsibility of the nations; however, there is a common understanding of what qualities are obligatory for the SOF operator. According to Eric Sof (2022), missions assigned to SOF are carried out by operatives trained to be agile and lethal when the situation calls for it. The SOF operator is specially selected, satisfies high training standards, is well educated, can operate cutting-edge equipment, and employs special skills, non-standard technics, and procedures to contribute to Special Operations.

AJP-3.5 describes SO as military actions executed by specifically selected, organized, trained, and equipped personnel employing unique methods and tactics. These efforts may be made alone or alongside conventional troops. Politico-military issues may entail covert operations and the assumption of political or military danger unrelated to regular troops. SO have strategic or operational implications or involve high political risk (NATO, 2019).

If to look directly, principal SOF tasks could be executed by conventional forces; for example, raids, ambushes, assaults, area or object reconnaissance, provision of training, and advice to local forces are standard everyday tasks for Land Forces. However, the employment of SO has allowed for the completion of tasks that

conventional troops were either unable to complete or unable to do with a degree of risk deemed acceptable (Soli, 2021).

Nations like Belgium, France, Great Britain, and the United States of America have their own SOF doctrines. There could be differences, including differentiation in the list of principal tasks such as contribution to Homeland Defense or Close Protection (CP) operations. However, due to the NATO standardization process, member states' doctrines differ in small ways (Rob de Wijk et al., 2021).

Chapter 2. SOF in the state-on-state conflict. Drivers for change

During the last decade, military interventions to support the international legal order became less relevant. SOF must prove its value on the modern battlefield and its central role in collective defense and internal security (Rob de Wijk et al., 2021). That said, there is an unquestionable requirement for change: to be prepared to fight against the adversary, most likely coming in extensive formations and maintaining the advantage of the firepower. Thus, the potential doctrinal changes, roles, tasks, and effectiveness of SOF employment in the contemporary battlefield became an excellent discussion and research topic among military experts, including doubters of the SOF's role in a conventional war. To contradict negative opinions, there is a need to look back and discuss the SOF’s effectiveness during World War II and analyze the Ukrainian SOF's performance on the contemporary battlefield, fighting against the armed forces of the Russian Federation.

2.1. Special operations during WWII

SOF units were effectively employed and tremendously contributed to the overall success of the battles, operations, and campaigns during WWII. According to Horn (2018), special units were created to compensate for weaknesses and satisfy special requirements that regular troops needed to be deemed more cumbersome or insufficiently prepared to meet. They tied thousands of enemy troops for defensive attacks, captured strategic materials such as Wurzburg radar components and Enigma encryption materials, destroyed enemy items and infrastructure, halted the German

nuclear weapon program, and raised, trained, and outfitted, and in some cases led, secret armies and resistance networks.

If to look closer at the provided facts from the perspective of AJP-3.5, we can easily recognize that SOF during WWII has been ordered to exercise its principal tasks, which execution complemented conventional forces and contributed to operational and strategic goals; however, tactics and the means employed during the WWII in some cases have been different to compare with modern SOF. Thus, the case of the Ukraine war must be analyzed to prove that NATO SOF doctrinal tasks are valid and that SOF is an invaluable tool on the contemporary battlefield.

2.2. Special operations in the war in Ukraine

The Ukrainian SOF actions in the war with the Russian Armed Forces bring solid facts and lessons learned to confirm that SOF is a significant contributor to operational success. UKR SOF is a force multiplier and provides Ukraine's Armed Forces with specialized capabilities designed to fill essential shortages in important military sectors (Borsari, 2022). They have already proven that SOF can effectively fight against the enemy with a significant quantitative superiority while executing three NATO SOF principal tasks and additional activities; UKR SOF was prepared to employ a combination of guerrilla tactics, direct actions, and unconventional warfare methods against a quantitatively superior enemy (Dieanu, 2022).

At this point, it is essential to remember that before the war, UKR SOF had been trained by several NATO member nations SOF, including Baltic States, Canada, Poland, the United Kingdom, the United States of America, and others, with NATO SOF Headquarters effort coordination and synchronization role, focusing on developing UKR SOF's capabilities to execute SR, DA, MA missions in different environments following doctrinal requirements. Below provided facts reflect the effectiveness of SOF while running DA and MA tasks in the contemporary fighting environment.

Units of Ukrainian SOCOM conducted aggressive activities behind enemy lines, which resulted in the destruction of some command posts and the death of numerous critical leaders in the Russian Federation invading forces' chain of command. Among the

successful missions of the UKR SOF is disrupting the enemy logistic flow; also training and organizing resistance cells for guerrilla warfare within Russian-occupied Ukrainian territories (Dieanu, 2022).

It is more complicated to find evidence regarding reconnaissance operations. Due to understandable reasons, information regarding UKR SOF special reconnaissance operations appears outside of open sources. Moreover, in most cases, SR is a critical phase of DA operations, providing necessary information for successful target neutralization.

Analysis of the Ukrainian SOF actions in the war against the Russian Federation helps to understand potential requirements for NATO SOF doctrinal changes. It will significantly impact the current understanding of the Modus Operandi and future structures of the NATO nations SOF (Dieanu, 2022). It becomes evident that SOF activities such as utilizing networks, organizing resistance, and sabotage operations are necessary to remain effective while fighting aggressors like the Russian Federation. It's also important to remember that development is primarily about dynamics within present tasks, not adding new tasks to the doctrine.

Chapter 3. Special Reconnaissance

3.1. SR role and support to the Joint Force

Military commanders at all levels employ reconnaissance to dispel the fog of war and fill the existing gaps in their comprehension of the battlefield. It is and will continue to be a significant component of understanding & shape efforts in all kinds of armed conflicts (Rob de Wijk et al., 2021). Moreover, gaining political approval depends on provided information (Watling, 2021). Conventional forces reconnaissance formations conduct reconnaissance operations depending on the operational requirements; however, once it comes to strategic information or politically sensitive environments, special operations troops are employed to perform SR. According to Watling (2021), bridging knowledge gaps becomes crucial when critical information is lacking. Strategic reconnaissance requires SO units to get the needed answers.

AJP-3.5 defines SR as reconnaissance and surveillance undertaken as an operation in hostile, denied, or diplomatically and politically sensitive contexts to acquire or verify strategic or operational intelligence conducted by SOF utilizing distinctive tactics and methods. Activities within SR can include (1) Environmental Reconnaissance, (2) Threat assessment, (3) Target assessment, and (4) Post-action reconnaissance (NATO, 2019).

SOF has been executing the task of SR in low-intensity conflicts but moving to the state-on-state conflict environment, SOF utilization while conducting strategic reconnaissance gets additional importance. Rob de Wijk et al. (2021) state that SR is needed to assist deployed troops, engage Russia, understand and shape the battlefield, and prepare for asymmetric deterrence by collecting information on Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance ((C4ISR) – joint battle management system) equipment and military locations, support decision-making processes, and provide intelligence for proxy forces.

SR could be assessed as one of the most significant SOF principal tasks. Collected high-value intelligence information significantly contributes to and supports Joint Force Commander's or Battle Space Owners' intent and contributes to the desired effects. Watling (2021) states that long-distance patrols and covert operations in highly populated areas differ from special forces' war on terror efforts. Special forces may become the Joint Force's most vital enabler.

3.2. SR and Clandestine Operations

The typical Intelligence, Surveillance, and Reconnaissance most militaries used in Iraq and Afghanistan have become outmoded, and SOF must adapt to contemporary warfare (Ball, 2023). They must modify their mentalities, methods of operation, and instruments meant for counterterrorism and counterinsurgency operations to the large-scale fight against the state aggressor (Watling, 2021). This sub-chapter focuses on the SR principle of *cover*, particularly the clandestine SR operations, as the proposed effective way of operating on the contemporary battlefield.

The four SR principles of *review, cover, reporting, and exploitation* have been brought by Anders Westberg (2016). Considering that most SOF operations will be conducted in urban terrain and densely populated regions, the need to blind in the local environment to perform clandestine SR operations plays a crucial role. Former US Undersecretary of Defense for Intelligence, Dr. Michael Vickers, states that we are the hunted once inside this environment. We are tracked in a manner that we have never been before. Facial recognition, digital and DNA footprints, and a more significant profile make it far more difficult to maintain anonymity in an information-dense setting. Thus, strategy and tactics must evolve. Every entry, operation, and resupply of equipment must alter (Taft et al., 2019).

According to the theory, the cover has numerous levels. Two subsets exist inside the cover principle. The first includes topography, climate, disguise, cover story, and camouflage. This research focuses on "cover for action," which describes the collecting unit's genuine function. The collecting team must blend in with the local population and employ cross-cultural communication skills to avoid being discovered (Westberg, 2016).

That said, SOF units must develop tactics, technics, and procedures to be ready for the execution of clandestine, potentially long-term SR operations in highly populated areas. Exercises must be organized in civil urban terrain, allowing SOF operators to train and develop their abilities in the environment reflecting realistic, modern battlefield conditions. AJP-3.5 states that political and military factors may necessitate clandestine operations. It defines them as operations planned or conducted to assure secrecy or concealment (NATO, 2019); however, the document does not define and discuss clandestine SR. Considering the increased actuality of low visibility or clandestine intelligence collection, clandestine SR operations could be a valid subject for further analysis and potential inclusion into the NATO SOF doctrine.

Another factor significantly contributing to intelligence gathering in the contemporary environment is the *network.* A well-developed network ensures a solid intelligence reporting system and attitudes of the local population and governmental and non-governmental institutions. Intelligence gathering relies heavily on the SOF's focus on contacts and network development (Taft et al., 2019). When tensions increase, SOF's

most significant role is a developed network in place; an in-depth comprehension of the adversary's thinking process and techniques are necessary (Taft et al., 2019). However, networking is more related to the other NATO SOF core task - MA, and terms of resistance operations, total defense, and force integration. It will be discussed in the next chapter.

Chapter 4. Military Assistance

4.1. MA role and support to the Joint Force

Military Assistance as a military task could be conducted by conventional forces and units of special operations forces; the difference is that SOF is usually focused on the internal or external entities of strategic and operational importance (such as national CT units, SOF, Police SWAT units, etc.). Moreover, the perception of this task could also vary depending on the country's size and policies. For example, in most cases, MA, from the perspective of crisis management operations and big nations' view, is focused on the support (train, advise, assist, accompany) provided to external actors. According to US JP-3-05, MA is an integral part of Foreign Internal Defense (FID), which is described as a state's civilian and military agencies participating in the other government's or designated body's action plans to protect the populace from subversion, anarchy, and insurgency (JCoS, 2003).

In parallel, the NATO SOF doctrine provides an MA definition that could be more applicable for internal usage, focused on "critical friendly assets," and could be executed while organizing the national defense. The provided definition of MA is SOF actions and activities that assist, empower, and influence critical friendly assets via training, advising, mentoring, and partnering. MA activities may include (1) Training, (2) Advising, (3) Mentoring, (4) Partnering; (5) Interagency Support (NATO, 2019).

MA operations have played a significant role and contributed to achieving operational objectives in Crisis Management operations, but the task acquires even more considerable attention in the contemporary environment. Although not all operational and higher-level military leaders are willing to utilize the benefits that well-developed and battle-tested SOF competencies could create, there are a few fields where SOF

could be employed in the context of today's battlefields and contribute significantly to JF efforts. However, doctrinal additions are required to extend the MA definition with the term Networking activities. Rietjens and Zomer (2018) illustrate the statement by stating that one of the aspects of the SOF's effectiveness is the ability to build networks. Networks are effectively utilized in gathering intelligence information, influencing the attitudes of the local population, and ensuring effective communications and logistical support.

4.2. MA and Network building

Being decades-long and involved in low-intensity conflicts, the gained experiences significantly contribute to the contemporary situation. SOF plays a vital role in understanding the battlefield by collecting information and establishing and maintaining networks with the local population and officials (Rob de Wijk et al., 2021). However, AJP-3.5 does not distinguish network building as a separate activity within MA; the doctrine focuses on neutralizing the enemy networks rather than defining and emphasizing the importance of developing its networks for intelligence gathering and effective MA execution in the contemporary environment.

Considering the context of modern threats: adversaries' intelligence and detection capabilities, the ability to generate and employ mass troops, and the possibility of partial or complete occupation (which cannot be ruled out) of the country lead to the necessity to consider the importance of (1) force preservation and the necessity of force multiplication, (2) the SOF's role in organizing the whole of society's defense while providing the necessary mentoring to the identified entities of the resistance operations, and (3) ability of the adequate provision of the liaison with allied and conventional forces. All three must be integral to effective network building under MA operations.

First, we must consider that, in most cases, a small nation has limited resources. Armed forces are proportional to the size of the country and population; consequently, the smaller NATO nations have conditionally small numbers of qualified SOF operators: some of the NATO countries have less than 300 combat-ready troops. Thus, every loss on the battlefield could significantly hamper the overall capacity of the

execution of the SOF operations, and the preservation of force acquires significant importance. Fighting against adversaries with numerical and firepower advantage, SOF must find ways to preserve the force and remain effective in the execution of the given missions during all the phases of the conflict, starting with the initial response to the enemy's incursion to the resistance, in case if the national defense fails. One proposed solution would be utilizing a well-developed network with the potential pool of forces to be trained and employed on the battlefield when required. The collection of troops could consist of selected units from the regular forces, voluntary forces, reserves, members of paramilitary organizations, or even people having membership in hunting or paintball clubs. Utilizing unique technics of vetting, monitoring, training, and trust and relationship building gained during the decades-long participation in crisis response operations would help to generate and keep a significant number of forces available for a time if a crisis occurs. In this case, SOF would act as a force multiplier generating and lately employing enough well-prepared forces to achieve operational effects and preserve the SOF capabilities for the extent of the conflict. Stringer (2022) provides an example of force multiplication, a 12-person US SF Operational Detachment A (ODA) can train, advise, and help an entire irregular or territorial defense force battalion, according to the doctrine. This skill enhances the impact of a limited number of special forces troops across the area of operations.

Secondly, SOF operators and units should be trained and capable of organizing and leading small formations and developing a network for resistance actions in case of partial or complete occupation of the country. NATO SOF doctrine defines Military Assistance through the train, advice, assist, accompany (TAA(A)) concept but does not include network-building (organizing formations of active fighters, establishing logistical and medical support nodes, ensuring linkages with external entities) as a factor essential for the effective execution of the resistance. Stinger (2022), in his article Special Operation Forces: The Integrators for Total Defence and Resistance also, states that Special Operations Forces have the expertise for resistance as part of their UW capabilities and experience in integrating law enforcement, intelligence, and other agencies; but they lack the mass and countrywide presence needed to lead and perform national resistance activities effectively. However, the second part of the statement is arguable, considering that access to the group and a more comprehensive presence could be a part of effective network building, especially using SOF's

developed flexibility and ability to engage multi-layer authorities and establish relationships with various entities in the area of operations. All the mentioned are inseparable parts of the effective execution of the resistance through well-developed networks.

Lastly, effective integration of JF elements and other critical actors on the battlefield plays a significant role in the nowadays fighting environment, where networking as a part of MA activities could play an important role. There SOF might come to play and operate as perfect integrators and contribute significantly to the assurance of unity of effort by creating connections between essential elements on the battlefield. Canadian BG Hunter (2021) provides that SOF acknowledges that they will be required to execute a vital role in strategic competition. Partnerships and operational connections with JF components, other government entities, and allies will become of utmost importance for SOF's capacity to integrate with other military and security entities. Future military operations against peer enemies will need an increasingly tighter partnership between SOF and conventional troops (Stringer, 2022).

Summing up, SOF’s decades-long MA and networking experience gained in crisis response operations could be used in the contemporary environment. If wisely employed, SOF operators, as integrators, force multipliers, or resistance organizers, are invaluable JF commanders’ tools in the execution of joint operations. Therefore, the doctrinal definition of MA should be revised, considering the importance and SOF’s ability to build and utilize networks.

Chapter 5. Direct Actions

5.1. DA role and support to the Joint Force

SOF units can significantly contribute to the JF Commander's desired effects by conducting operations to eliminate High-Value Targets or other objects of high importance. Historical cases and examples from the war in Ukraine of SOF-conducted raids contributing to achieving operational or even strategic goals have been provided in the previous chapters of this paper. Brands and Nichols (2020) offer a perfect example of how strategic raids could neutralize critical elements of an adversary's

A2AD system, allowing a more significant force to continue operating with greater flexibility or to remove a target that would otherwise consume a considerable number of scarce munitions, such as precision-guided, standoff missiles, that are desperately needed elsewhere. The strategic raid might also provide a method for attacking critical adversary capabilities, infrastructure, personnel, or weaknesses in a relatively stealthy manner. This tactic may appeal to policymakers fearful of needless escalation.

NATO SOF Doctrine defines DA as a short-duration SOF operation or other small-scale offensive to seize, destroy, capture, recover, or inflict damage to accomplish well-defined, typically time-sensitive goals. DA can include (1) Raids, ambushes, and assaults, (2) Terminal guidance operations, (3) Recovery operations, and (4) Precision destruction operations (NATO, 2019). The direct actions, not only raids, could contribute to the campaign's overall success if the SOF units were utilized wisely and professionally.

Nevertheless, there are opponents of the SOF's effectiveness in the modern, contemporary battlefield. Hooker (2023) states that commandos do not help countries win wars. Regardless of its proponent's claim, light-armed SOF groups cannot seize and hold territory and cannot produce decisive strategic outcomes. Neither are they tangible economy-of-force assets; as we have shown, their costs in terms of money and personnel do not correspond with their actual contributions to the operation's success. Contrary to provided, the general truth has to be considered that SOF is not competing but complimenting other elements of the JF and supporting them where is required and possible; however, looking from the smaller nations' perspective, and again considering potential adversary quantitative, and firepower advantages, execution of AJP-3.5 defined DA tasks, especially raids, ambushes, and assaults getting in direct contact with opposing force units could cause conditionally fast exhaustion of SOF forces making their contribution to the operational success hardly possible. Thus, additional ways of operating on the contemporary battlefield must be analyzed and implemented into NATO SOF Doctrine. The option to maintain Admiral McRaven's essential principles of success of SO - simplicity, security, repetition, surprise, speed, and purpose (McRaven, 1996) while preserving the force available to the greatest extent possible could be Sabotage operations, which are not included in the current version of the AJP-3.5.

5.2. Sabotage operations

Analysis of Sabotage operations must be commenced by defining and understanding the terms of Irregular Warfare (IW) and Unconventional Warfare (UW). There is no doctrine-based definition of IW. Eriksson (2017) describes it as a different military mentality that employs ways other than conventional warfare to exhaust and erode the opponent's will or a comprehensive strategy used to win the war by methods other than traditional combat. The definition enables the tiny state to use a vast array of designs. For example, it comprises hit-and-run tactics, avoiding conflict, and any confrontation when casualties are imminent. However, nations tend to use the doctrinal definition of UW and Sabotage operations defined by US Joint Publication 3-05 (JP-3-05), just adapting them for internal operations.

JP-3-05 describes UW operations as a broad variety of military and paramilitary actions, usually long-term, primarily conducted by indigenous or proxy soldiers organized, trained, equipped, backed, and directed by an external source. The biggest misconception about UW is the understanding that it is limited to guerrilla warfare and insurgency. UW includes but is not limited to, the following activities: (1) Guerrilla Warfare, (2) Subversion, (3) Sabotage, (4) Intelligence Activities, and (5) Unconventional Assisted Recovery (JCoS, 2003).

The same publication defines Sabotage operations as an act or actions aimed at harming, interfering with, or impeding a country's national defense by intentionally damaging or neutralizing, or trying to injure or destroy, national defense or war material, premises, or utilities, including human and natural resources (JCoS, 2003). Sabotage targets enemy capabilities with minimum resources. It is part of UW, which aims across all stages of armed conflict to exploit the weaknesses of the enemy and cause disruption in its systems. Operations may have to complement traditional DA against opposing forces to engage the opposite state's Centers of Gravity (Rob de Wijk et al., 2021).

Gallagher's "The Attack in Norway" perfectly illustrates the effectiveness of Sabotage operations and how small SOF formations can contribute the strategic success; in

February 1944, an assault team member of a secret unit called the Special Operations Executive sabotaged and sunk a boat transporting two train carriages of heavy water to Germany over a deep lake. The operation effectively ended Germany's strategic nuclear weapon development. Hitler then moved his scientists to focus on the V1 and V2 rockets, which, as history has proven, had little impact on the United Kingdom's capacity to wage war and only served to strengthen the will of the British people (JCoS, 2003).

Sabotage could be one of the most effective ways of employment of national or NATO SOF units (not necessarily as a part of Resistance or Guerrilla Warfare activities) to support the Joint Force Commander's objectives and aim at the enemy's targets of significant importance with a minimum force required; however, NATO AJP-3.5, contrary to US JP-3-05, does not include UW either as a SOF task or activity and mentions it only in the context of Personnel Recovery Operations as an Unconventional Assisted Recovery, defined as special operations recovery missions using pre-established indigenous networks.

Conclusions and Recommendations

The research confirms that SOF remains a valuable and effective tool for achieving Joint Force objectives, especially in areas with high political sensitivity or operational risks. The current geopolitical situation dictates the need for NATO to be able to ensure speed of recognition and decision to react to a crisis adequately (Hodges et al., 2020), and there will always be the necessity to neutralize the enemy’s High-Value Targets if the situation escalates to the armed conflict; thus valid options to employ SF operators to support decision-makers and accomplish actions directly contributing to the achievement of operational effects always exist. Moreover, the outstanding performance of the Ukrainian SOF during the ongoing Russian invasion has already proved that SOF has a vital position in the broad spectrum of warfare on the contemporary battlefield.

Another research-confirmed factor is that SOF conducts activities throughout its classic tasks. Regardless of the change of threat nature, the execution of three principal tasks,

SR, MA, and DA, defined by the Allied Joint Doctrine for Special Operations, remains relevant (Rob de Wijk et al., 2021). However, they must be revised and adapted to current threats and requirements of the contemporary battlefield. Looking at the issue from a small nation's perspective, the context of modern threats, particularly the adversary's quantitative and firepower superiority, must be considered, and tasks adapted to the current situation within available capabilities and existing limitations.

SOF must remain flexible while changing its focus from counterterrorism and man-hunting operations to fighting against state-aggressor. Refocusing SOF is both required and appropriate, and if correctly integrated with theatre and campaign planning, SOF may contribute significantly to the campaign's success (Hooker, 2023). So, the SOF community is realigning, and units are adapting their tactics and technics procedures within the framework of principal tasks and finding the most effective ways to complement conventional forces and contribute to achieving JF objectives. Ability to blend in local populations and conduct prolonged clandestine SR operations, the importance of developing networks to ensure force preservation and multiplication, integration function, and organizing networks to support resistance movements in case of the country falls under partial or complete occupation, and finally, being small and light and still capable of impacting adversary's objects of significant importance are proposed changes to be considered for adaptation of principle SOF tasks.

The analysis leads to the following recommendations: firstly, the NATO SOF community at all levels should periodically and more often review and, if needed, initiate the adjustments of the doctrine, implementing the best practices and available Lessons Learned from the contemporary battlefield in Ukraine, also considering adversary's developments in doctrine, tactics, procedures, and capabilities, as well as the impact of technological progress and innovations. Secondly, constructive, subject matter expert-supported discussions to decide on the requirements for doctrinal changes are necessary, emphasizing the differences and finding the consensus between big and small nations of the Alliance. Thus, the following recommendation is for the NATO Special Operations Forces Headquarters (NSHQ), the primary coordinator of NATO SOF activities and development. NSHQ should ensure that NATO SOF doctrine is universal and reflects the needs and requirements of both big and small nations to be effective on the contemporary battlefield. Based on provided

research results, proposed AJP-3.5 adjustments should be further analyzed and considered for implementation: (1) extend SR and MA definitions with networking activities, (2) define and include clandestine ways of conducting SR as a Special Operations Task Group capability requirement, (3) expand DA task with Sabotage Operations as a way for the “David against Goliath” fight. Lastly, doctrinal changes, capabilities, mission sets, techniques, and procedures should be tested with realistic scenarios during national and NATO exercises, as well as included in the NATO Special Operations School (NSOS) curriculum to unify and develop the understanding of NATO SOF community and partners on the changes in SOF roles, capability requirements, and the ways to remain effective in contemporary military conflict.

Bibliography

Ball Tim. 2023. Managing Risk for Special Operations Forces in Large-Scale Combat Operations. *War on the Rocks*. [Online] 21 February 2023. [Cited: 25 March 2023]. https://warontherocks.com/2023/02/managing-risk-for-special-operations-forces-in-large-scale-combat-operations/.

Borsari Federico. 2022. Hunting the Invader: Ukraine's Special Operations Troops. *Cepa*. [Online] 15 March 2022. [Cited: 27 March 2023]. 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, August 2020.

Counter-currents Collective. 2022. Ukraine Update: NATO to rethink of Europe Force Stance. [Online] 23 March 2022. [Cited: 25 March 2023]. https://countercurrents.org/2022/03/ukraine-update-nato-to-rethink-of-europe-force-stance/.

De Wijk Rob, Bekkers Frank, Sweijs Tim, De Spiegeleire Stephan, Kool Dorith. 2021. The Future of NLD SOF: Towards an All-Domain Force. The Hague: Hague Centre of Strategic Studies, July 2021.

Dieanu Adrian - Corneliu. 2022. The Role of Ukrainian Special Operations Forces within the War in Ukraine. Carol I, the National Defence University of Bucharest.

Eriksson Gunilla and Pettersson Ulrica. 2017. *Irregular Warfare – A Strategy for Small States?* Special Operations from Small State Perspective. New Security Challenges. Stockholm: Palgrave Macmillan, 2017.

Hodges Ben, Lawrence Tony, and Wojcik Ray. 2020. Report – Until Something Moves**.** International Centre for Defence and Security, April 2020.

Hooker D. Richard, Jr. 2023. America's Special Operations Problem. *Joint Force Quarterly*. 1st Quarter 2023, Issue 108.

Horn Bernd. 2018. *The evolution of SOF and the rise of SOF Power.* CASS Military Studies. Special Operations Forces in the 21st Century. Perspectives from the Social Sciences. New York: Routledge, 2018.

Hunter Steve. 2021. CANSOFCOM: A Leader's Perspective on Great Power Competition and SOF. *Kingston Consortium on International Security Insights*. November 2021, Vol. 1, Issue 7.

Joint Chiefs of Staff (JCoS) 2003. US Joint Publication 3-05. Doctrine for Joint Special Operations. Washington, DC.

Maass Matthias. 2009. The elusive definition of the small state. *International Politics*. January 2009, Vol. 46, 1.

McRaven H. William. 1996. Spec Ops: Case Studies in Special Operations Warfare: Theory and Practice, Novato CA: Presidio Press, 1996.

NATO. 2022. NATO 2022 Strategic Concept adopted by Heads of State and Government at the NATO Summit in Madrid.

NATO Standardization Office (NSO). 2019. NATO Allied Joint Publication. AJP-3.5. Allied Joint Doctrine for Special Operations. Edition B Version 1.

Pettersson Ulrica and Ilis-Alm Hans. 2022. Resistance Operations: Challenges and Opportunities for Special Operations Forces. *Journal on Baltic Security*. 2022, 8(1).

Rietjens Sebastiaan and Zomer Jelle. 2018. *The Dutch Special Forces in Mali. In Search of Intelligence.* CASS Military Studies. Special Operations Forces in the 21st Century. Perspectives from the Social Sciences. New York: Routledge, 2018.

Sof Eric. 2022. Special forces and their role in the history of warfare. *Spec Ops Magazine* [Online] 29 April 2022. [Cited: 25 March 2023]. https://special-ops.org/special-forces-in-history-of-warfare/.

Solli Bjørn-Erik. 2021. The Essence of Special Operations. What You Need to Know About Special Operations while Serving at the Joint Operational Level. NATO Joint Warfare Center. *The Three Swords Magazine*. 37/2021.

Stringer D. Kevin. 2022. Special Operations Forces (SOF): The Integrators for Total Defense and Resistance. *Journal on Baltic Security*, *Resistance Operating Concept, Special Issue.* Volume 8 (1).

Taft John, Gormizky Liz and Mariani Joe. 2019. Special operations forces and great power competition. Talent, technology, and organizational change in the new threat environment. Deloitte Center for Government Insights. [Online] 17 June 2022. [Cited: 25 March 2023]. https://www2.deloitte.com/content/dam/insights/us/articles/4980_special-operations-forces/DI_special-operations-forces.pdf.

Titulaer Funs. 2021. Special operations (forces) explained. On the nature of Western special operations and the forces that conduct them. *Military Spectator*. [Online] 12 February 2021. [Cited: 25 March 2023]. https://militairespectator.nl/artikelen/special-operations-forces-explained-0.

Watling Jack. 2021. Sharpening the Dagger. Optimising Special Forces for Future Conflict. Royal United Services Institute for Defence and Security Studies. Whitehall Report 1-21. [Online] 27 May 2021. [Cited: 25 March 2023]. https://static.rusi.org/whr_special_forces.pdf.

Westberg Anders. 2016. To See and Not to Be Seen: Emerging Principles and Theory of Special Reconnaissance and Surveillance Missions for Special Operations Forces. *Special Operations Journal*, July 2016.

MAJ Jurijs KAZENKO. Is the development of new military technology an opportunity or a threat to Latvia's security?

Introduction

For a small state like Latvia, survival and maintenance of national security in a world of large, capable military powers means being intelligent and practical economically, politically, militarily, and socially. These prerequisites for success can be achieved through modern technology development and implementation in small but flexible armed forces. The most recent worldwide warfighting trends and identified lessons have shown the necessity for technologically advanced military forces' performance in all battlefield domains. In the war of attrition, states' inability to sustain a numerically significant army can be balanced through military technological advancement. The author of this paper will debate the contemporary controversies about the development of new military technology and its role in national security.

Working through the military capability development process, it is essential for a small state to consider multiple aspects and factors, like new technological innovations, current and future technological market and security development trends, as well as the corresponding potential political, economic, and security risks. In addition, a state should assess and consider how new technology can aid in defending against an asymmetric adversary. New technologies should be adopted gradually and intelligently to ensure a country's national and international security requirements.

Developing new military technology can present opportunities and challenges for a small state. To use new technologies to their advantage, the administration of an analytically complex and bureaucratically challenging development and implementation process requires a comprehensive approach, smart tactics, the development of clear strategies, and methodological support for decisions.

Despite an optimistic vision and potential gain, new technologies are not always beneficial. Technological development can also create challenges for a small state

depending on substantial conditions. While it may increase state security, technological development can also lead to significant social and economic issues, bringing the state budget to the point of exhaustion or posing new risks to public safety. A small state's security sector governance must be proactive in ensuring its security sector is pacesetting to mitigate strategic dependencies that can complicate the development of new military technology. Moreover, developing new technology for a small state must be a collaborative effort that results in more advanced capabilities.

Even though the development, ownership, and maintenance of modern and sophisticated military equipment are highly costly, whether Latvia is a part of the NATO alliance or fights on its own, it must maintain modern, capable, and interoperable armed forces. To elaborate on the given statement, the author will narrow down the scope and focus the analysis on the Air Force as being the most reliant on technology for capability improvements in the security sector.

This paper will argue that although the development of new military technology may cause a threat of technological dependence or increase the possibility of cyberattacks, it is certainly an opportunity to strengthen the state’s national security by building technologically advanced but affordable defensive capabilities with high levels of interoperability, improved data analysis and decision support. Moreover, this paper will assess the benefits and possible detriments of developing new military technology for countries such as Latvia by utilising local science and industry to the maximum extent possible and leveraging relationships with political and military allies.

The research paper is structured into six sections: background, NATO, Latvia, SWOT Analysis, recommendations, and conclusions at the end of the paper. The first section sets the basis and scopes the environment for further analysis. The following sections provide insight into the technological scope and future trends of NATO and Latvia, as well as the possible air capability requirements for Latvian Air Forces. The following SWOT analysis is used in this research paper to evaluate the Strengths, Weaknesses, Opportunities, and Threats of the military technological development environment in Latvia. Possible solutions to meet the needs of the future development of the Latvian Air Force are presented in the recommendations. Lastly, the conclusion offers a complete summary of the research paper.

Background

Military technology has evolved significantly over the past century, from the introduction of aeroplanes and tanks in World War I to computer-controlled drones and cyberwarfare in the present. Advances in military technology became possible due to developments in communications technology, weapons systems, and electronic warfare (Yoo, 2017). Technology has played a significant role in how wars are fought. Introducing new tools and tactics has allowed for increased effectiveness and precision on the battlefield. Aside from this, applying science to warfare has also led to the developing of new weapons and strategies, which have positive and negative impacts on global security.

Throughout the years, military technology has become a broad and complex field of study that encompasses a wide range of subjects, including the development of new weapons and equipment, the application of technology in combat, the analysis of its effects on military operations, and warfare changing nature (Billing, et al., 2021). The technological advancements militaries use to enhance and expand their capabilities demand research for new communication and armament systems, intelligence-gathering techniques, surveillance instruments, and ways of applying robotics and artificial intelligence in military operations (Czapla, et al., 2013). This also necessitates a closer examination of the relationship between civilian and military activities and the positive or negative effects the military imposes on the civilian population by applying new technologies to meet the demands of contemporary warfare (Hoffman, 2009, pp. 34-39).

Military technology has always had a significant effect on society. In terms of political, social, military, and economic implications, innovations transform the way societies interact, from international politics to individual lifestyles (Pianta, 1988). Accordingly, it is impossible to entirely separate civilian and military activities; in times of peace, conflict, or war, both will be engaged in constant interaction. For example, dual-purpose technology, from microwaves to GPS and the Internet, has found a home in both civilian and military uses, giving rise to a new era of technological innovation (Thompson, 2022).

Nowadays, civilian applications are often leading the way in advancing new technology. Previously, military technologies had been at the forefront of technological advancement as governments sought to gain an advantage in warfare. This shift has been driven by the increasing availability and affordability of powerful computing hardware, software and other components that can be used for civilian and military purposes (Kaminski, 1995). This alteration has resulted in a much closer relationship between civilian and military technological advancement than ever before. Civilian applications are often used as a foundation for further research and development by the military, which can then adapt existing technology for their unique use cases (Harris, et al., 2016). For instance, autonomous drones are now commonplace in commercial air travel and military operations due to advances in drone technology originating from civilian projects. Similarly, artificial intelligence is being used to improve surgical techniques and automate certain aspects of warfare, such as target identification (SDi, 2023).

The close relationship between dual-use technologies creates an environment where there is less distinction between civilian and military applications, allowing both sectors to benefit from advances made on either side (SDi, 2023). This increases overall efficiency and effectiveness and creates opportunities for collaboration between different organisations. Furthermore, it inevitably changes society's perceptions of war, its impacts on civilian populations, and the power dynamics between countries (Cao, et al., 2020). Ultimately this shift could lead to a world where dual-use technologies are so intertwined that it becomes difficult to distinguish between civilian or military applications ushering in a new era of technological advancement for all.

Military technology has a significant and far-reaching impact on international relations due to its potential to create instability or even conflict between countries (Lieber, et al., 2017). Developments in military technology have enabled states to project power over greater distances than ever before. This has been seen in recent years as countries like China and Russia have used advanced military technologies, such as long-range missiles, to expand their influence beyond their borders (Heginbotham, 2015). The potential of nuclear weapons to cause destruction on an unprecedented

scale led to mutual deterrents such as Mutually Assured Destruction (MAD) (Muller, 2004, pp. 13-15).

Similarly, technological innovations in unmanned aerial vehicles (UAVs) or unmanned combat aerial vehicles (UCAVs) provide not only a new dimension and opportunities for warfare but also raise concerns about the potential for autonomous decision-making and the ethical implications of using such technology in conflict situations. Their use during military operations in Iraq, Afghanistan, and the ongoing war in Ukraine, has allowed states to conduct precision strikes without putting personnel at risk. These innovations have tactical effects protecting the operators' lives and strategic impact in terms of deterrence (Ven Bruusgaard, 2016).

Consequently, the new military technology has a significant deterrence effect. It increases the cost of waging war on potential aggressors and makes it much more difficult for them to achieve their goals (Scheipers, 2018). Furthermore, potential adversaries are now more aware of the capabilities of other militaries, which has forced potential adversaries to consider the risks and consequences of any aggressive action before deciding whether or not to initiate hostilities (Lieber, et al., 2017). Lastly, it increases transparency and communication between countries, which can help build trust and discourage conflict.

Indeed, military technology has transformed how wars are fought, and organisations interact. It has influenced the development of dual-use technologies, changed the nature of warfare, and impacted global relations. The evolution of military technology is ongoing, and it is up to governments to ensure that these technologies are used responsibly and ethically to control the proliferation of weapons and maintain international stability (Ven Bruusgaard, 2016, p. 15).

As Winston Churchill once said in this well-known quote: "There is only one thing worse than fighting with allies, and that is fighting without them" (Alanbrooke, et al., 2001). Therefore, the following section will provide an overview of NATO technology scope and future trends to understand how NATO can assist Latvia, as a NATO member, in achieving its goal of becoming a capable partner in the alliance, increasing efficiency and gaining international recognition.

NATO

Across the Atlantic, nations increasingly turn to innovative technologies to build stronger and more resilient armed forces. These technologies are opening up new dimensions for warfare and transforming the security environment in which NATO operates. While NATO is strengthening, a new wave of disruptive technologies is reshaping our daily lives, representing new threats from state and non-state actors. Adapting to this new wave of technology and hazards caused by technological development will help NATO militaries become more agile and effective (NATO, 2022).

The integration of cutting-edge technological solutions into NATO's operational strategy and defence against potential threats has been a significant challenge for NATO forces (NATO Forces Interoperability, 2018). Research and development have allowed for the evolution of NATO's technology capabilities to meet increased operational demands over time. As a result, the Alliance has identified seven technological components that are essential for maintaining its strategic edge against potentially equivalent military powers as Russia and China: standardisation, network-centric warfare (NCW), cybersecurity, unmanned systems, autonomous systems, data fusion and artificial intelligence (AI) (Reding, et al., 2020).

Accordingly, to build a technologically adaptive, nimble, and resilient alliance, NATO has scoped its future trends. In NATO, future technology envelops artificial intelligence (AI), distributed ledger technologies (DLT) and blockchain technologies, cloud computing and virtualisation, big data analytics and machine learning, autonomous robots and drones, geospatial technologies such as the Geographic Information Systems (GIS) and the Global Navigation Satellite System (GNSS) (Reding, et al., 2020; Bendett, 2022). Additionally, NATO will increasingly focus on space-based capabilities, including satellite communications and navigation (Burbach, 2022). Finally, 5G networks are expected to become increasingly important in the near future for military operations. Moreover, these technologies must function effectively as dual-use technologies that can be used in civilian and military capacities (Boling, et al., 2022).

To summarise, the scope of NATO technologies, combined with the future trends being explored, provides Latvia with a solid foundation to grow and become a reliable partner

in the alliance. Close cooperation with allies prevents the adverse effects of strategic misalignment created by a strategic imbalance in the region when introducing new military technology may put a country at odds with its neighbours. Implementing and adopting cutting-edge technologies and equipment will enable Latvian Air Force to protect its airspace from state and non-state actors, improving the self-defence capabilities of the state (Rule, 2015).

For further analysis, it is essential to examine Latvia's national technological vision and trends and investigate the Latvian Air Forces' air capability requirements. This will lead to the definition of the strengths, weaknesses, opportunities, and threats for the analysis aiming to identify and distinguish the positive or negative impact on the security of Latvia.

Latvia

The vision of national military technological development in Latvia is described and specified in the State Defence Concept. Approved by the Cabinet of Ministers on August 18, 2020, and adopted by the Saeima on September 24, 2020, the State Defence Framework is based on five central pillars: the National Armed Forces, the Comprehensive Defence System, NATO collective defence, international cooperation, the European Union, and the state defence assets (Milevski, 2020). Based on these five central pillars, the government defines the ends, means, and ways to develop and maintain the necessary technology and capabilities to ensure the development of the country’s defence (MOD, n.d.).

The aim is for Latvia to develop a modern, professional, capable defence capability with modern weapons systems, equipment, and technology that supports a credible and effective deterrence posture and denies potential aggressors. Further, since Latvia shares border with powerful and potentially hostile countries such as Russia and Belarus, which could lead to increased vulnerability (Lamoreaux, et al., 2008), advanced military technology could improve Latvia’s deterrence against hostile actions through the provision of capabilities to respond to threats and demonstrate the commitment to use them if necessary (Andžāns, et al., 2017). To this end, the Latvian Armed Forces seek to acquire high-tech weaponry from NATO partners and develop a comprehensive cyber defence system. Additionally, Latvia will continue its military

research and development efforts to keep up with the ever-changing security environment and future technological trends (Ministry of Defence, 2020).

The national technological trends of Latvia are focused on developing the country's digital infrastructure, encouraging the use of modern technologies, and advancing research and innovation (Menaker, et al., 2018; OECD, 2021). The emphasis on the local industry adopting the technology will become an essential tool for the Latvian Air forces to modernise and improve their capabilities in upcoming years. This includes providing components, systems, and services that enable the Air Force to be more effective and efficient.

Latvia is looking forward to fostering a culture of innovation and collaboration between the private sector, academia, and national military institutions to ensure sustainable economic growth and national security. Therefore, Latvia must invest in research and development to foster innovation, which will help boost the national industry's growth and competitiveness. Additionally, a collaboration between different sectors can lead to the creation of novel technologies that can contribute to the modernisation of the Latvian Air Force (GlobalData, 2022). Furthermore, developing new technologies can help strengthen international ties as foreign countries could be interested in acquiring these innovations. This can lead to increased trade between countries and improved diplomatic relations.

The local economy will gain financially from supplying technologies to the military, allowing them to increase their business opportunities (Menaker, et al., 2018, p. 161). Local companies are to become instrumental in supporting the Air Force’s effort to improve capabilities and prepare for potential security threats by providing communications systems, surveillance equipment, navigation systems, sensors, and unmanned aerial vehicles (UAVs) (Stein, 2022). By working together, both parties will ensure the implementation of modern technology while boosting the economy through increased demand for goods and services. Moreover, investing in military technology can create jobs and boost economic growth. As resources are allocated towards research and development of new technologies, more people are employed in the industry, leading to increased economic activity (Ruttan, 2006).

Current global security concerns influence future Air Force development trends in Latvia, with the war in Ukraine serving as the primary focal point (Latvian Army, 2023). Forecasts of events and lessons identified determine the future design and modernisation requirements of the Air Force, including air mobility, search and rescue, ground-based air defence, command and control, cyber defence, early warning, and training capabilities (Masulis, 2020). In addition, the armed forces foresee the necessity of developing counter-drone systems and unmanned aerial vehicles (UAVs) based battlefield management, intelligence, surveillance, and reconnaissance systems (Latvian Army, 2023). Regarding specific initiatives, Latvia invests in developing 5G technology, artificial intelligence, and blockchain applications (Nikers, 2020).

However, science and industry development demand substantial financial, time, and human resources. High cost of research and production, in combination with affordability, limited access to resources and a fragile economic situation, can cause significant negative economic and social effects. To maintain a credible and effective defence posture, a state might concentrate on developing its military capability based on the open global market, which could result in technological dependence and unforeseen risks (Bellais, 2013). These factors make military technology expensive and difficult for many countries to afford. The cost of maintaining these technologies can also be substantial due to the need for specialised personnel and equipment (Anderton, 2022).

The current geopolitical and economic situation has presented challenges for all air forces worldwide. It is now their top priority to optimise organisations and operations to meet national security requirements better while putting new capabilities into service (Kainikara, 2009). Even though the basic provisions for security across the globe remain the same, the size of the forces is determined by the state's geopolitical location, the perceived threat level, and – most importantly – the size of the national budget (Skogstad, 2016). As a result, state officials must determine the Latvian Air Force's military air capability requirements. Furthermore, the joint acquisition permits nations to maximise the effectiveness of their defence investments and coordinate their defence resources, promoting regional stability and security (Hankewitz, 2022). Therefore, the small states should choose a comprehensive regional approach for the major military procurements.

Due to geopolitical and economic reasons, Latvian air forces can afford only essential air capabilities and cannot compete with the air forces of bigger and wealthier countries. It is necessary to remember that the air force's quality, not its size, determines its success in defensive and offensive operations (Beckley, 2010). Quality, however, requires continuous investment in training, maintenance, and modernisation of equipment, which can be challenging for small states with limited resources. In this context, the *prioritised* Latvian Air Force capability requirements include providing air surveillance, enabling allies and partners to operate and control the airspace, and conducting air defence, tactical reconnaissance, and search and rescue missions (Masulis, 2020). Capabilities that are able to conduct air-to-air or air-to-ground combat missions are not part of the prioritised capability requirement list due to the high cost of the associated air platforms, weapons, ammunition, and their maintenance (Roblin, 2021).

As a strategic planning tool, the SWOT Analysis will be used in this research paper to evaluate the Strengths, Weaknesses, Opportunities, and Threats of the military technological development environment in Latvia. Previously recognised and aforementioned strengths include the commitment to modernising technologies, cooperation with allies and the emphasis on the local industry in the adoption of technology. Weaknesses include a fragile economic situation, limited access to resources, and the high cost of research and production. Opportunities include enhanced deterrence, increased business opportunities for local companies and the potential for collaboration between different sectors to create novel technologies. Threats include technological dependence and unforeseen risks associated with open global markets. The careful consideration of these elements is essential to ensure the successful development and implementation of new technology in the Latvian Air Force.

SWOT Analysis

The SWOT Analysis in this section will provide a framework to identify and assess internal and external environments to understand if the development of new military

technology is an opportunity or a threat to Latvia's security. For this analysis, only the most important factors will be considered and assessed (Table 1).

Table 1.

Strengths	Weaknesses
1. Political will and support 2. Local science 3. Cooperation with allies 4. International Recognition 5. Developed military infrastructure	1. Cost / Affordability 2. Limited Access to Resources 3. Limited access to funds for research and development 4. A fragile economic situation 5. Lack of public awareness
Opportunities	**Threats**
1. Utilising local science and industry 2. Increasing Deterrence 3. Promoting Economic Development 4. Investing in modern communications and cyber security technologies 5. Enhancing existing weapon systems 6. Developing unmanned aerial vehicles (UAVs)	1. Cyber threat 2. Technological Dependence 3. Operational depth / Survivability 4. Proliferation of Weapons 5. Unforeseen Risks 6. Strategic Misalignment

New military technology can help to strengthen Latvia's defensive capabilities by providing more effective weaponry, better communication systems, and improved surveillance and battlespace management technology (NATO, 2022). These advancements enable the Latvian Air Force to improve and maintain airspace control, increase situational awareness (SA) and enhance command and control capability, providing the ability to respond quickly and effectively. Military technology can provide air forces with more accurate and timely data, facilitating better decisions. For example, advanced sensors and communication systems can gather real-time information about the battlefield environment, allowing commanders to make decisions faster and more accurately. Additionally, AI-driven analytics engines can help analyse vast amounts of identification data to recognise patterns indicating threats or opportunities that would otherwise go unnoticed.

Military technology is expensive to develop and acquire due to the complexity and high equipment, materials, and labour cost. Therefore, the production of big areal platforms

in Latvia is highly limited due to the limited access to funds for research and development as well as limited or non-existent resources or infrastructure necessary to produce complex equipment. The state may not have access to advanced computer systems, software, specific components or materials like wolfram, titanium or aluminium used to produce certain military technologies. It forces the local industry to search for and adopt alternative composite materials for light aeroplanes, unmanned aerial vehicles, and communication systems (ESA, 2021; Kokorevičs, 2021). Therefore, Latvia has to show political will and utilise governmental support to the local academia and industry to stimulate and consolidate the effort in the development of national military technology.

The state defence framework in Latvia has to support the industry by providing access to government funding, research opportunities, and technical assistance. These initiatives include tax incentives, the establishment of a defence industry cluster, and export promotion programs. Automation and robotics can also reduce the need for manual labour from foreign countries. In this way, military technology investments can help increase the efficiency of operations within the country, create a more stable economy, and maintain a competitive advantage that will result in technologically advanced but affordable products.

Emerging new military technology domestically allows Latvia to save on acquiring foreign technologies and raise cost-effectiveness while allowing for customising its military technology to its own needs and specifications. Additionally, as depicted in Figure 1., using local science and industry offers the country Strategic Autonomy and the ability to become self-sufficient and independent from foreign sources for its defence needs (Crespi, et al., 2021; Helwig, et al., 2021). In theory, it encourages innovation and investment within the local economy, creates jobs and stimulates economic growth. However, the benefit over the off the shelf procurements has to be evaluated on the governmental level (Berg, et al., 2017).

Apart from this, enhancing existing weapon systems can improve the performance of legacy weapon systems that Latvian Air forces operate. Enhanced safety features added to existing weapons systems help prevent operations-related hazards and increase safety. Enhancements increase reliability and durability; the system will last

longer and perform better over time. It also makes it more interoperable or adaptable to new scenarios or threats in response to changing conditions (NIC, 2021). Despite Latvia having entirely discarded all legacy military equipment from the Soviet era and gradually replaced it with more contemporary Western equipment (LSM.lv, 2023), partnership with NATO and rapid technology development forces Latvian Air forces to invest in the upgrade of the existing systems.

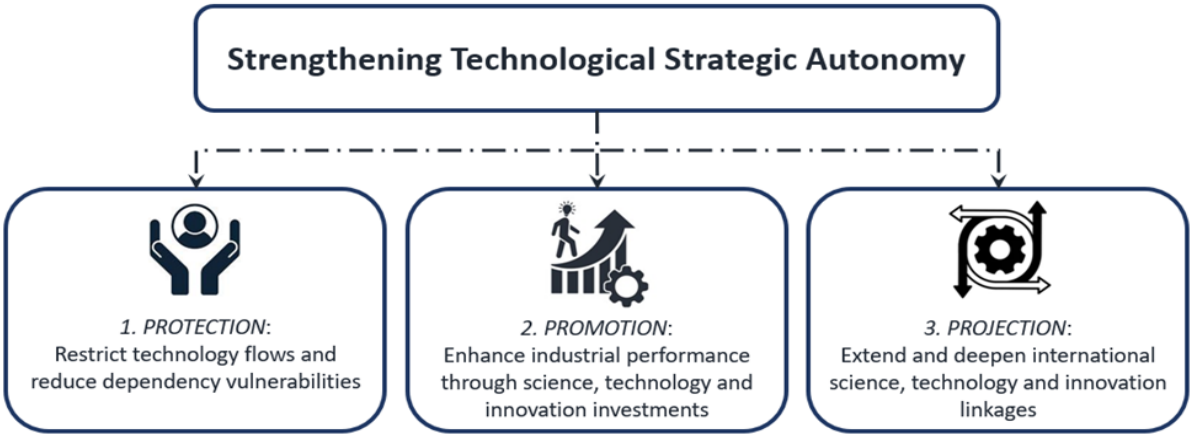


Figure 1. Three methods of increasing strategic autonomy. Source: (Helwig, et al., 2021, p. 13).

Technological collaboration with NATO nations provides Latvia with higher levels of interoperability through a common set of technology standards and protocols and a better understanding of the battlefield environment. For example, computer-based Improved Data Analysis and Decision Support Systems help organisations to process large amounts of data, identify patterns, recognise trends, and develop insights to form decisions. These systems use AI, machine learning, predictive analytics, and natural language processing techniques to analyse vast amounts of data from multiple sources (Davis, et al., 2004). Provided that Latvia has access to a wide range of cutting-edge, most up-to-date military technologies that can be used to enhance its security posture (Welscher, 2022). It ensures that Latvian Air forces are able to effectively operate within NATO on a more consistent basis.

On the contrary, developing new military technology can increase the cyber threat for Latvia in several ways. First, as Latvia effectively develops its military technology, it may create more access points for malicious actors to exploit. For example, the Latvian armed forces have a successful cooperation with the local communication company

“Latvijas Mobilais Telefons” (LMT). If the Latvian Air forces adopt new 5 G-supported technologies, these systems could be vulnerable to hacking and manipulation. Moreover, developing new military technology can create a "target-rich environment" where the military may inadvertently reveal vulnerabilities that hackers and other malicious actors can exploit (Lester, et al., 2020). These risks could lead to significant costs and disruption if an attack were successful (Nikers, 2020).

Another possible drawback of military technology development in Latvia is its limited operational depth. Latvia’s security situation is threatened by hostile neighbouring powers such as Russia and Belarus, which could launch an attack against Latvia at any time. In case of attack, military technology infrastructure becomes a prioritised target for the adversary. Knowing the capabilities of contemporary long-range kinetic effects, the operational depth of Latvia becomes a significant complication for the state’s defence (Ekholm, 2021). Therefore, the potential locations of the military technology infrastructure, limited by operational security, must be evaluated, designed and constructed, considering all precautions. Moreover, Latvia has to have the necessary resources (personnel, equipment, and technology) to ensure military industry sites are protected in case of an attack and be able to detect and respond to any attack promptly (Brown, et al., 2014). Finally, maintaining strong relationships with NATO allies is essential for supporting a successful defence against hostile foreign powers.

Overall, Latvia seeks to take advantage of technology’s opportunities while mitigating potential threats. By investing in research and development and collaborating with the private sector, academia, and military institutions, Latvia is working to develop a modern and capable defence capability with available resources. Additionally, by focusing on air capability requirements such as Air Command and Control (AirC2), air surveillance, air defence, tactical reconnaissance, and contribution to battlespace management, Latvia is capable of creating a credible deterrence posture without overstretching its resources.

Recommendations

The following recommendations are based on the analysis of Latvia's initial steps to innovate and strengthen its defence capabilities, the overarching NATO development trends and the SWOT analysis of the military technological development environment in Latvia.

First of all, for the development of the industry within the state defence framework, Latvia needs to keep implementing policies and initiatives that support the growth of the domestic defence and security industry and foster close relationships with its stakeholders. Clear national priorities are necessary for effective and meaningful support of industry development. The development of the National Armed Forces' capability and the potential of the national economy must serve as the foundation for these priorities.

Second, one of the state initiatives must be creating a national innovation support framework to promote innovation and research development, with the potential for integration into EU and NATO scientific programmes. The growth and competitiveness of the national industry depend heavily on innovation. Despite constraints resulting from resource limitations faced by the sector, effective transfer and implementation of innovative technologies will significantly increase the Latvian Armed Forces' capacity to deliver in terms of state defence.

Small states can refine the range of new military technologies developed by the public and private sectors while preserving their monopoly over force. In addition to being aware of the development of new military technology, Latvia should also invest in its local science and industry to ensure that it is able to take advantage of modern military technology and reduce technological dependence. This would include investing in local universities, research centres, and defence companies so that Latvia would develop a local base of expertise in modern military technology. This would allow Latvia to build its advanced technologies for use by its air force and other branches of the armed forces improving self-defence and increasing deterrence capability. Additionally, Latvia could gain international recognition by investing in the local industry.

Even though it is anticipated that by 2025, Latvia's defence spending will reach 2.5% of its gross domestic product (ERR News, 2023), it must also be conscious of the monetary risks connected to research and development endeavours and the adoption of technological innovations. As was stated by Sean McFate, "the worth of any weapon is its utility," meaning that before investing significant funds into any project, the state must undertake a thorough analysis to ensure that it will contribute to the resolution of current and future technological challenges (The Heritage Foundation, 2019). Consequently, measures to support innovation must align with national priorities and produce novel, ground-breaking technologies in industries with higher national research and development potential. Moreover, small states must have the courage and ability to cancel major projects if necessary. The costs of strategic miscalculation are high, especially when the size of the state budget is limited and less flexible.

Finally, Latvian Air Forces should consider adopting civil-military dual-use technology to improve the efficiency and effectiveness of its military capabilities. This can include the incorporation of existing commercial technologies, such as IA, 5G, robotics, Unmanned aerial vehicles and systems, data analytics and other technologies, into military operations. By taking advantage of existing technologies, Latvia can reduce the cost and time spent on the development of new military technologies while still achieving the desired level of combat readiness.

Conclusions

After a thorough analysis, it became evident that the developing new military technology has the potential to strengthen national security by providing defensive capabilities that are technologically advanced but affordable, with higher levels of interoperability. Moreover, new military technology gives states a better understanding of the battlefield and its tactical environment. Thus, Improved Data Analysis and Decision Support Systems allow for more precise analysis and decision-making in less time. This can help states prepare for potential conflicts or take preventive measures before they occur.

This primarily benefits countries like Latvia, which must rely on limited resources and political alliances to protect themselves from external threats. Developing new military

technology could potentially involve leveraging local science and industry for the research and production of goods. This could create job opportunities, stimulate economic growth and improve the country's technological infrastructure. It would also reduce reliance on foreign suppliers, increasing self-sufficiency in defence.

On the other hand, there may be some drawbacks to developing new military technology in Latvia. For instance, there is always a risk that such development will be perceived as an escalation of military power or create conditions for cyber-attack by hostile states or groups. Furthermore, the costs associated with developing and acquiring new military technology can be prohibitive for a small state like Latvia. Investing heavily in defensive capabilities may result in a neglect of social welfare issues or other economic sectors, which could result in an economic decrease in the country. Ultimately, each country must carefully weigh the advantages and disadvantages before deciding whether or not to pursue new military technology development projects. However, it is clear that, driven by supportive national security policies, such projects could provide valuable benefits if implemented correctly. Additionally, Latvia's security is threatened by its limited resources and operational depth. Therefore, careful consideration must be given to the available resources and strategies for developing new military technology to ensure that it benefits Latvia's security in the long term.

In general, NATO is leading the way in developing cutting-edge technologies for use in its defensive operations. Air power technologies are revolutionising warfare and providing NATO a strategic edge over its adversaries. The Alliance's research, technological innovation, and increased operational requirements provide the military with the tools to protect its airspace and improve its capabilities. By integrating new, innovative technological solutions into its strategy, NATO is helping countries like Latvia to become more agile and effective in their operations. These technologies enable Latvian Air Force to become a reliable partner in the alliance while ensuring they are adequately prepared for potential threats from state and non-state actors.

To conclude, while new military technology may pose a threat in certain circumstances, it is a definite opportunity for states to strengthen their national security with advanced defensive capabilities at an affordable cost. Such technology will provide greater

interoperability and allow for better analysis and decision-making when dealing with potential conflicts or asymmetric attacks. The key to ensuring that the development of new military technology is an opportunity rather than a threat lies in careful planning, strategic investment, and collaboration with NATO allies to ensure that the Latvian Armed Forces can effectively use the latest technologies available. The Latvian Armed Forces also seek new opportunities to adopt dual-use technology, prioritising the local industry. By focusing on these developments, Latvia will ensure its military technological development while boosting its economy through increased demand for goods and services.

Bibliography

Alanbrooke, Alan, Danchev, Alex and Todman, Daniel. 2001. *War diaries, 1939-1945.* Berkeley : University of California Press, 2001. p. 725. 0-520-23902-4.

Anderton, James. 2022. How Military Aircraft Engines Got So Expensive. *Engineering.com.* [Online] September 02, 2022. [Cited: February 7, 2023.] https://www.engineering.com/story/how-military-aircraft-engines-got-so-expensive.

Andžāns, Māris and Veebel, Viljar. 2017. Deterrence Dilemma in Latvia and Estonia: Finding the Balance between External Military Solidarity and Territorial Defence. *Journal on Baltic Security.* 2017, Vol. 3, 2, pp. 29-41.

Beckley, Michael. 2010. Economic Development and Military Effectiveness. *Journal of Strategic Studies.* February 1, 2010, Vol. 33, 1, pp. 43-79.

Bellais, Renaud. 2013. Technology and the defense industry: real threats, bad habits, or new (market) opportunities?:. *Journal of Innovation Economics & Management.* June 1, 2013, Vol. 12, 2, pp. 59-78.

Bendett, Samuel. 2022. The Ukraine war and its impact on Russian development of autonomous weapons. *Atlantic Council.* [Online] Atlantic Council, August 30, 2022. [Cited: February 22, 2023.] https://www.atlanticcouncil.org/content-series/airpower-after-ukraine/the-ukraine-war-and-its-impact-on-russian-development-of-autonomous-weapons/.

Berg, Helene, Ofstad Presterud, Ane and Øhrn, Morten. 2017. Military Off the Shelf Procurements: A Norwegian Case Study. *Defence and Peace Economics.* June 19, 2017, Vol. 30, pp. 1-13.

Billing, Daniel C., et al. 2021. The implications of emerging technology on military human performance research priorities. *Journal of Science and Medicine in Sport.* October 1, 2021, Vol. 24, 10, pp. 947-953.

Boling, Bryan, et al. 2022. Emerging technology beyond 2035: scenario-based technology assessment for future military contingencies. Santa Monica : RAND Corporation, 2022. p. 118. 978-1-977409-99-7.

Brown, Gerald G., et al. 2014. Analyzing the Vulnerability of Critical Infrastructure to Attack and Planning Defenses. *TutORials in Operations Research.* s.l. : INFORMS, 2014, pp. 102-123.

Burbach, David T. 2022. Early lessons from the Russia-Ukraine war as a space conflict. *Atlantic Council.* [Online] Atlantic Council, August 30, 2022. [Cited: February 22, 2023.] https://www.atlanticcouncil.org/content-series/airpower-after-ukraine/early-lessons-from-the-russia-ukraine-war-as-a-space-conflict/.

Cao, Xia, Yang, Xiaojun and Zhang, Lupeng. 2020. Conversion of Dual-Use Technology: A Differential Game Analysis under the Civil-Military Integration. *Symmetry.* November 12, 2020, Vol. 12, 11, p. 1861.

Crespi, Francesco, et al. 2021. European Technological Sovereignty: An Emerging Framework for Policy Strategy. *Intereconomics.* November 2021, Vol. 56, 6, pp. 348-354.

Czapla, Tomasz and Wrona, Józef. 2013. Technology Development of Military Applications of Unmanned Ground Vehicles. [ed.] Aleksander Nawrat and Zygmunt Kuś. *Vision Based Systemsfor UAV Applications. Studies in Computational Intelligence.* Heidelberg : Springer International Publishing, 2013, Vol. 481, pp. 293-309.

Davis, Paul K., Kulick, Jonathan and Egner, Michael. 2004. Modern Decision Support Science Suggests New Methods and Tools to Support Military Decisionmaking. *Project Air Force.* Santa Monica, California, USA : RAND Corporation, January 1, 2004.

Ekholm, Anders. 2021. Re-thinking operational depth—A source of power. *Comparative Strategy.* July 4, 2021, Vol. 40, 4, pp. 387-406.

ERR News. 2023. Latvia follows Estonia's lead in boosting defense spend, to 2.25% of GDP. *ERR.* [Online] Eesti Rahvusringhääling, March 11, 2023. [Cited: March 14, 2023.] https://news.err.ee/1608911984/latvia-follows-estonia-s-lead-in-boosting-defense-spend-to-2-25-of-gdp.

ESA. 2021. Greener polyurethanes for space and beyond. *The European Space Agency.* [Online] January 14, 2021. [Cited: March 21, 2023.] https://www.esa.int/Enabling_Support/Space_Engineering_Technology/Greener_polyurethanes_for_space_and_beyond.

GlobalData. 2022. Latvia Defense Market Size and Trends, Budget Allocation, Regulations, Key Acquisitions, Competitive Landscape and Forecast, 2022-2027. *Market Research Reports & Consulting.* [Online] GlobalData UK Ltd., November 10, 2022. [Cited: March 19, 2023.] https://www.globaldata.com/store/report/latvia-defense-market-analysis/.

Hankewitz, Sten. 2022. Estonia plans to acquire a mid-range air defence system with Latvia. *Estonian World.* [Online] July 15, 2022. [Cited: March 25, 2023.] https://estonianworld.com/security/estonia-plans-to-acquire-a-mid-range-air-defence-system-with-latvia/.

Harris, Elisa D., Acton, James M. and Lin, Herbert. 2016. Governance of Dual-Use Technologies: Theory and Practice. *American Academy of Arts and Sciences.* [Online] April 2016. [Cited: March 18, 2023.] https://www.amacad.org/publication/governance-dual-use-technologies-theory-and-practice/section/3. 0-87724-110-4.

Heginbotham, Eric. 2015. The U.S.-China Military Scorecard: Forces, Geography, and the Evolving Balance of Power, 1996-2017. Santa Monica, CA : RAND, 2015. p. 389. 978-0-8330-8219-0.

Helwig, Niklas, et al. 2021. *Strategic autonomy and the transformation of the EU: New agendas for security, diplomacy, trade and technology.* FIIA. Helsinki, Finnland : Finish Institute of International Affairs (FIIA), 2021. p. 136. 978-951-769-682-1.

Hoffman, Frank G. 2009. Hybrid warfare and Challenges. [ed.] David H. Gurney. *Joint Force Quarterly.* 2, January 2009, Vol. 1st Quarter 2009, 52, pp. 329-355.

Kainikara, Sanu. 2009. *The Future Relevance of Smaller Air Forces.* Canberra : Royal Australian Air Force. Air Power Development Centre, 2009. p. 14. 978-1-920800-42-0.

Kaminski, Paul G. 1995. Dual Use Technology - European Security. *EUROPEAN SECURITY.* [Online] European-Security, May 17, 1995. [Cited: March 15, 2023.] https://european-security.com/dual-use-technology/.

Kokorevičs, Arnis. 2021. Article about LSIWC investigations in the portal of European Space Agency. *Latvian State Institute of Wood Chemistry.* [Online] LSIOWC, January 28, 2021. [Cited: January 12, 2023.] http://www.kki.lv/en/latest-news/article-about-lsiwc-investigations-portal-european-space-agency.

Lamoreaux, Jeremy W. and Galbreath, David J. 2008. The Baltic States As 'Small States': Negotiating The 'East' By Engaging The 'West'. *Journal of Baltic Studies.* March 1, 2008, Vol. 39, 1, pp. 1-14.

Latvian Army. 2023. Video: Seminar on the National Defense Concept "Cornerstones of National Defense". *Sargs.lv.* [Online] Sargs.lv, 16 March 2023. [Cited: 19 March 2023.] https://www.sargs.lv/lv/nozares-politika/2023-03-16/video-seminars-par-valsts-aizsardzibas-koncepciju-valsts-aizsardzibas.

Lester, Phil and Moore, Sean. 2020. Responding to the Cyber Threat: A UK Military Perspective. *Connections: The Quarterly Journal.* 2020, Vol. 19, 1, pp. 39-44.

Lieber, Keir A. and Press, Daryl G. 2017. The New Era of Counterforce: Technological Change and the Future of Nuclear Deterrence. *International Security.* April 1, 2017, Vol. 41, 4, pp. 9-49.

LSM.lv. 2023. NAF commander: Latvia has completely abandoned Soviet-era military equipment. *LSM.lv.* [Online] February 24, 2023. [Cited: March 12, 2023.]

https://www.lsm.lv/raksts/zinas/latvija/nbs-komandieris-latvija-ir-pilniba-atteikusies-no-padomju-laiku-militaras-tehnikas.a497959/.

Masulis, Viesturs. 2020. Air Force Commander: For development to be strong, it must be synchronized. [interv.] Sargs.lv. *Opinion.* March 6, 2020.

Menaker, Joseph and Ozoliņa, Velga. 2018. Latvian High-Tech Industry: Trends and Developments. *Economics and Business.* July 1, 2018, Vol. 32, 1, pp. 160-171.

Milevski, Lukas. 2020. Latvia's New State Defense Concept. *Foreign Policy Research Institute.* [Online] June 25, 2020. [Cited: February 20, 2023.] Section: Baltic Bulletin. https://www.fpri.org/article/2020/06/latvias-new-state-defense-concept/.

Ministry of Defence. 2020. *The State Defence Concept of Latvia.* Riga, Latvia : MOD, September 24, 2020.

MOD. n.d.. Defence policy. *Ministry of Defence Republic of Latvia.* [Online] n.d. [Cited: October 27, 2022.] https://www.mod.gov.lv/en/nozares-politika.

Muller, Richard R. 2004. *Getting MAD: nuclear mutual assured destruction, its origins and practice.* [ed.] Henry D. Sokolski. Carlisle, PA : Strategic Studies Institute, 2004. p. 361. 978-1-58487-172-9.

NATO. 2022. Emerging and disruptive technologies. *North Atlantic Treaty Organization.* [Online] NATO, December 8, 2022. [Cited: January 27, 2023.] https://www.nato.int/cps/en/natohq/topics_184303.htm.

NATO Forces Interoperability. **Popescu, Eugen. 2018.** Bucharest : "CAROL I" National Defence University, 2018. International Scientific Conference "Strategies XXI", suppl. Strategic Changes in Security and International Relations. Vol. 2, p. 122.

NIC. 2021. *Global Trends 2040: A More Contested World.* Washington, D.C. : National Intelligence Council, 2021. p. 156. 978-1-929667-33-8.

Nikers, Olevs. 2020. 5G Technologies in Latvia Advance Military Capabilities and National Economy. *Jamestown.* [Online] December 15, 2020. [Cited: February 19, 2023.] https://jamestown.org/program/5g-technologies-in-latvia-advance-military-capabilities-and-national-economy/.

OECD. 2021. *Going Digital in Latvia.* Paris : OECD Publishing, 2021. p. 236. Vol. OECD Reviews of Digital Transformation. 978-92-64-55190-9.

Pianta, Mario. 1988. *New technologies across the Atlantic: US leadership or European autonomy?* 1. publ. Hemel Hempstead : Wheatsheaf [u.a.], 1988. p. 170. 978-0-7450-0442-6.

Reding, D. F. and Eaton, J. 2020. *Science & Technology Trends 2020-2040: Exploring the S&T Edge.* NATO Science & Technology Organization. Brussels, Belgium : NATO Science & Technology Organization, 2020.

Roblin, Sébastien. 2021. Opinion | Air Force finally admits the F-35 is too expensive. Its solution? Spend even more. *NBC News.* [Online] NBC, March 19, 2021. [Cited:

January 20, 2023.] https://www.nbcnews.com/think/opinion/air-force-admits-f-35-fighter-jet-costs-too-much-ncna1259781.

Rule, Troy A. 2015. Airspace in an age of drones. *Boston University Law Review.* September 2015, Vol. 95, 155, pp. 155-208.

Ruttan, Vernon W. 2006. *Is war necessary for economic growth? military procurement and technology development.* Oxford : Oxford University Press, 2006. p. 219. 978-0-19-518804-2.

Scheipers, Sibylle. 2018. *On Small War: Carl von Clausewitz and People's War.* Oxford : Oxford University Press, 2018. p. 222. 978-0-19-251981-8.

SDi. 2023. The Most Useful Military Applications of AI in 2023 and Beyond. *Sentient Digital, Inc.* [Online] Sentient Digital, Inc, January 2023. [Cited: March 15, 2023.] https://sdi.ai/blog/the-most-useful-military-applications-of-ai/.

Skogstad, Karl. 2016. Defence budgets in the post-Cold War era: a spatial econometrics approach. *Defence and Peace Economics.* May 3, 2016, Vol. 27, 3, pp. 323-352.

Stein, Aaron . 2022. The TB2: The value of a cheap and “good enough” drone. *Atlantic Council.* [Online] Atlantic Council, August 30, 2022. [Cited: February 05, 2023.] https://www.atlanticcouncil.org/content-series/airpower-after-ukraine/the-tb2-the-value-of-a-cheap-and-good-enough-drone/.

The Heritage Foundation. 2019. *The New Rules of War: Victory in the Age of Durable Disorder.* [perf.] Sean McFate. The Heritage Foundation, 2019.

Thompson, Maureena . 2022. Army modernization investments foster development of dual-use technologies. *U.S. ARMY.* [Online] Army Futures Command, May 12, 2022. [Cited: March 15, 2023.] https://www.army.mil/article/256647/army_modernization_investments_foster_development_of_dual_use_technologies.

Ven Bruusgaard, Kristin. 2016. Russian Strategic Deterrence. *Survival.* 3 July 2016, Vol. 58, 4, pp. 7-26.

Welscher, Alexander. 2022. How the Baltic countries are guarding against tough times. *Baltic Business Quarterly.* November 29, 2022, Vol. 4, pp. 26-29.

Yoo, John. 2017. Embracing the Machines: Rationalist War and New Weapons Technologies. *California Law Review.* 2017, Vol. 105, 2, pp. 443-499.

LDCR Andrew LATHROP. The EU engagement in Africa: Necessary task or a thankless endeavour?

Introduction

Europe and Africa share a long history of connectedness (EU-Africa, p.62). Today, Africa presents a nearly limitless source of opportunity for economic partnership and strategic growth for European nations to invest in. Conversely, Africa is a large and complicated structure that produces a nearly limitless number of challenges as well. The question thus arises, is the juice worth the squeeze? More concretely, do all the resources that the European Union and its member states pour into the continent in terms of money, time, military force, and political capital have the potential to yield satisfactory benefits?

Africa's rich abundance of natural resources, especially energy resources, make it a particularly high-value target for economic investment. Its population presents opportunities for additional trade markets, and its geography presents opportunities for powerful outside nations to establish both an economic and military footprint to project power.

African challenges for Western investments are myriad. For any investment in Africa to be viable, there must be some guarantee of security. At first glance, this seems impossible when facing overwhelming poverty, terrorism and violent extremism, rampant disease, masses of internally displaced persons and refugees, widespread corruption, illiberal democracies, war, famine, draught, and long-standing rivalries between states and peoples.

Popular phraseology regarding Africa revolves around the concept of "the nexus of security and development" (EPC 2007, p.1). The linkage between security and development requires that both are improved simultaneously. Investments require security to attract donors. Improving the security and stability of a region, however, will

require investment to meet the challenges and set the conditions for growth and prosperity.

Stakeholders in this discussion are not limited to the “Big 3” (France, Italy, Spain), nor to the body of the EU member states. Russia, China, the United States, and even Great Britain have their own agendas in Africa. And one must not lose sight of the agendas African nations have for themselves, and who rightly demand that their involvement in any partnership must be mutually beneficial, and respectful. Nonetheless, Europe cannot afford to miss opportunities to ensure its energy security, engage in cooperation to obtain new resources, compete on the global stage, enhance its security, and promote democracy and human rights in accordance with its values.

In this paper, I will first explain the impetus for European attention towards Africa and establish the potential for economic and strategic partnership in Africa. I will describe the major challenges that the EU has faced and will continue to face vis-à-vis security and development in Africa. Second, I will examine several of the proposals and recommendations from the past 2 decades on how the EU is approaching these challenges.

Next, I will then examine potential national and organizational interests related to Africa and categorize them as economic, strategic, or security-related opportunities. The analysis will cover EU interests in Africa from 3 different perspectives: 1) Economic Potential, 2) Strategic Competition, and 3) Security.
Finally, I will summarize the analysis and conclude by attempting to answer the questions: Why should the European Union continue to engage in Africa despite the setbacks and costs? And how might resources and effort be applied to produce a favourable outcome?

Background

The process by which European nations conquered practically the whole African continent as a component of their individual empires around the 1880s is generally referred to as the “Scramble for Africa”. Liberia and Ethiopia were the only two African nations who remained ungoverned by a European power by 1914. Through the process of colonialization in the scramble for Africa, the Europeans dramatically altered

the African continent. Most of Africa's affairs fell out of its own control. They fought numerous battles, experienced new diseases, and had their customary ways of life permanently altered. Over time, European nations relinquished power over their colonies, but they left behind many lingering issues. Ever since, the people of Africa have attempted to rebuild their economy and create independent, stable nations (Webster, Magdoff, Nowell 2022).

EU-Africa partnership in the 20th century began with the Treaty of Rome in 1957. This was the same treaty that established the European Economic Community, the predecessor organization of the European Union. This treaty provided a legal framework for European nations to partner with African ones, but this treaty was criticised by some African leaders as a “neo-colonial agreement”. Nonetheless, it provided the groundwork for future cooperation between Europe and Africa (EU-Africa, p.62-3).

Next came the Yaoundé Convention of 1969, which fell under similar criticisms and was replaced by a series of treaties known as the Lomé Conventions. These new conventions established a new basis for Euro-African partnership but continued to frustrate African leaders due to its fundamentally asymmetrical nature (EU-Africa, p.64). At the turn of the 21st century, the Cotonou Partnership Agreement (CPA), signed in June of 2000, established the modern partnership framework between the EU and Africa which is centred around the paradigms of mutual partnership and cooperation (EU-Africa, p.65).

The current agreements, and the history of their progression to date, clearly indicate that Euro-African partnership and cooperation are not going away any time soon. Researchers Forysiński and Emmanuel at the Eastern Mediterranean University in 2020 highlighted specific priorities proposed for the EU-Africa partnership as (Forysiński, Emmanuel 2020, p. 69):

- Achieving peace and stability
- Managing migration and mobility
- Consolidating democracy and good governance
- Unleashing economic opportunities
- Reaching human development standards
- Addressing climate change

Even while there are still many unanswered problems, African actors are becoming more supportive of a "continent-to-continent" collaboration with the European Union that would take advantage of Agenda 2063, the African Union's strategy to make Africa a global power. As researchers Forysiński and Emmanuel concluded in 2020: The integration of the EU-AU or AU-EU relationship into a single comprehensive framework is inevitable (Forysiński, Emmanuel 2020, p. 75).

The EU's triennial meeting with African states in February of 2022 saw the establishment of the Joint Vision for 2030, which focuses on solidarity, security, and sustainable prosperity (Sub-Saharan Africa 2022, p. 327). It is therefore clear that the EU is interested in achieving a long-term vision with partners in Africa. One problem, however, is that the member states of the EU struggle to speak with one voice when it comes to EU-Africa relationships (Adebajo, Whiteman 2012, p. 7).
Some examples of this disunity are:

1) French strategic documents clearly designate groups such as Islamic State and Boko Haram as national adversaries, and France has identified the Sahel and sub-Saharan Africa among the key regions in its strategic documents (Threat-based defence planning: implications for Canada 2021, p. 4).
2) Italy's geopolitical interest, however, focuses on the Mediterranean area, and NATO's southern flank (Threat-based defence planning: implications for Canada 2021, p. 6).
3) Northern Europe, by contrast, is seemingly disinterested in Africa, as evidenced by Norway's 2020 defence plan which disregards North Africa and the Sahel (Threat-based defence planning: implications for Canada 2021, p. 6).
4) Similarly, Sweden's focus on cooperation with Finland as a Strategic priority is adopted from a regional threat-based approach to strategic planning. They want little to do with African issues, at least from a military perspective (Threat-based defence planning: implications for Canada 2021, p. 8).

This lack of cohesion and resultant lack of unity of effort will inevitably lead to problems when competing with other interested parties (China, Russia) in Africa. Brussels must understand the priorities of its member states with respect to Africa in order to formulate a coherent policy (Witney, Dworkin 2012, p. 10).

Nevertheless, the EU-African connection is here to stay, at least for the foreseeable future, thus the task at hand should be to address the drawbacks while maximizing the

potential and benefits of a deal in the future (Forysiński, Emmanuel 2020, p. 68). What is common to EU member states is that the two arguments which dominate discussions on EU-Africa relations are: (1) the nature of the so-called neo-colonialist and exploitative relationship, and (2) general failure of African states to effectively govern (Forysiński, Emmanuel 2020, p. 70).

Analysis

In this section, I will discuss the probable European motivations for its interactions with and operations inside of African states. We will examine the EU-Africa relationship through several lenses. The first lens examines the economic ties between Europe and Africa. I will examine the relationship from the perspective of energy and non-energy resources in Africa which are valuable to the European continent. Then I will examine from the perspective of markets and trade. The second lens examines interests with respect to strategic competition and compares similar interests and approaches of the strategic competitors: China, Russia, and the United States. I will also discuss the ideological implications that pervade EU rhetoric. Through the third lens we will examine the relationship through the lens of security, which includes stability and migration.

Economic Potential

Resources and Energy

Africa is a largely untapped resource not only for oil and natural gas, but for non-energy related resources which have been deemed as ‘critical’ by the EU (Gerber 2012, p. 1). Logically speaking, the more critical the commodities that are produced by a region, the greater the significance of the region becomes (Gerber 2012, p. 9).

The security environment just across the Mediterranean Sea presents a significant challenge for Southern European countries from a perspective of energy security and supplies. Algeria, the largest supplier of energy resources in Northern Africa, has found a source of significant leverage when it comes to relationships it has with Morocco and Spain. Poor Algeria-Morocco relations and territorial disputes persist. Such struggles bleed into the energy sphere and manifest in a situation that is inconvenient for Spain, whose energy needs are met via the Medgaz pipeline which links Algeria and Spain,

as well as through liquefied natural gas shipping (Middle East and North Africa 2022, p. 293). Algeria's refusal to renew the Maghreb-Europe Gas (MEG) Pipeline and Spain's subsequent announcement that it intended to reverse flow of the MEG to Morocco caused Algeria to threaten suspending all gas supplies to Spain (Middle East and North Africa 2022, p. 293).

The energy situation in the region is further complicated by Russia's invasion of Ukraine in February of 2022 and the protracted war that has followed. This created a serious dilemma for European countries as they scramble to find alternative energy sources to Russian oil and gas. This has substantially increased Algeria's importance as an alternate energy supplier to Europe (Middle East and North Africa 2022, p. 294). Morocco presents a problem in this regard as well since it imports 90% of its energy needs, the bulk of which comes from coal imported from Russia (Middle East and North Africa 2022, p. 295). Algeria has gained diplomatic traction from Europe's search for alternatives to Russian energy sources (Middle East and North Africa 2022, p. 296). It is therefore quite clear that the security situation in North Africa's is in Europe's best interest to monitor closely and engage diplomatically and economically so as not to be held hostage by its own energy needs.

Markets and Trade

Africa's potential to open vast markets for European production has largely gone untapped by Europe. Instead of working to increase exports to Africa, Europe appears to be even reducing its engagement with African (particularly North African) markets. Europe has overlooked its potential partners on the other side of the Mediterranean in favour of the Middle East and beyond.

By 2007, Africa had already been neglected by the European agenda for many years (Kotsopoulos 2007). Less than 4% of the EU's external commerce has come from the North African states combined, even accounting for significant imports of oil and gas from Libya and Algeria (Witney, Dworkin 2012, p. 6). Few European countries have recently had any substantial links with North Africa, except for Italy, France, and Spain. Europe has omitted the North African region entirely, concentrating instead on the larger Middle East and sub-Saharan Africa (Witney, Dworkin 2012, p. 6).

Italy, France, and Spain have significant national interests at risk in terms of commerce, investments, and energy connections. They are also concerned about radicalization and terrorism and host the largest North African immigrant populations in Europe (Witney, Dworkin 2012, p. 7). Yet, their engagement activities seem to be lacking.

The EU accounts for 75% of sub-Saharan Africa's trade. By 2050, Africa is estimated to comprise a quarter of the global population (Cohen 2022). Yet, surprisingly, Africa is steadily becoming a much less important market for EU exports, imports and direct investments (Kotsopoulos 2007).

In 2018, African states had six of the world's ten fastest-growing economies. New African initiatives present lucrative prospects. Practical examples of such opportunities are the African Visa-Free trade area, the African Continental Free Trade Area, a single African Air Transport Market, and a single African Digital Market (Forysiński, Emmanuel 2020, p. 69).

To harness these opportunities, Europe must look outward and formulate a more generous, ambitious, and effective response to the upheavals in North Africa. Europe should also convince North Africa to understand European ideals and interests. This may require the council and EU member states to take on a more strategic view vis-à-vis Northern Africa (Witney, Dworkin 2012, p. 9).

Conclusion

Europe cannot afford to ignore the resource and market benefits that are possible through cooperation with Africa. Energy security and market growth will be vitally important for Europe in the years to come, and postponing African cooperation will prove troublesome in the future.

Strategic competition

What if Africa is simply the latest battleground on the world stage in which to wage war in global competition? If so, then a beneficial partnership between the EU and Africa is even more important given the growth of China as a key actor on the continent and the relevance of Africa as an alternative to the unstable Middle East as a source of oil and

raw commodities (Kotsopoulos 2007). Additionally, the presence of Russian paramilitary groups such as Wagner create friction for Europeans attempting to work cooperatively with governments in sub-Saharan Africa and the Sahel. After all, even friendly nations such as the United States present challenges like resource competition and potential for mis-coordination.

Historical and Colonial Ties

Several EU member nations (primarily France, Spain, Germany, and Belgium) have strong histories of colonial occupation in Africa. European nations' colonial ties in Africa create tensions with external relationship development between Europeans and Africans, but they create internal tensions as well in that European former colonial powers must work extra hard when formulating policies to avoid the perceptions of a revival of colonial attitudes towards resources on the African continent.

Europe is fortunate that it still has opportunities in Africa, and it must ensure that it is not too late to establish new partnerships and a relationship between the two continents that is truly equal and free of the baggage of the past (Adebajo, Whiteman 2012, p. 5). This matters today because France and other former colonial powers face an uphill battle in Africa, as their mere "neo-colonial presence" makes them a target of blame for the region's problems (Smith 2022, p. 9). These scars of colonialism, coupled with the liberal ideologies embedded in European rhetoric, create challenges for the EU.

China

Not only is China seeking fresh markets for its export-driven economy and ways to tap the wealth of natural resources in Africa, particularly energy supplies (Brookes 2007, p. 1), but its collection of interests (energy, trade, political, military) in Africa threaten Western efforts towards prosperity and democracy (Brookes 2007, p. 1). Beijing supports the finding of common ground with African partners by harping on the West's "overly moralizing, conditional and bureaucratic" tendencies (Brookes 2007, p. 3).

In particular, sub-Saharan Africa's lack of infrastructure poses a serious threat to its ability to develop for further growth and competition (Foster, Butterfield, Chen 2009, p. 74). This allows countries like China with enormous investment potential to target sub-

Saharan nations for predatory loans in order to develop infrastructure and establish more footholds in the region.

Largely, African governments tend to prefer China's modernization model to the challenging free-market and democratic changes advocated by the U.S. and the European Union because they are desperate to revitalize their faltering economies while still maintaining their firm hold on political power (Brookes 2007, p. 4). Through its pursuit of resources and influence, Beijing is certainly challenging the vision of free markets and democracy in Africa commonly held by European colonial and American partners (Brookes 2007, p. 5).

One risk for Western Democracies, in particular EU members (and the European Council itself), is that Africa's leaders, for the most part, prefer China's development assistance approach to that of the West, as it avoids interfering in state affairs and instead emphasises the state's participation (Gerber 2012, p. 2). Additionally, Chinese policies that support authoritarian regimes undermine the principles of EU initiatives in Africa (Brookes 2007, p. 1). This theme of combating authoritarianism and spreading democratic values in Africa poses a pervasive challenge for the West.

Another risk is that in lieu of genuine aspirations to secure access to mineral commodities and improve the material quality of life in sub-Saharan African nations, the significant emphasis and advocacy of EU rules and standards can be interpreted as attempts to merely preserve a European presence in the regions in place of that of the Chinese (Gerber 2012, p. 9).

Western nations are behind China when it comes to investment in Africa. Despite President Biden's pledge to the U.S.-Africa Leaders' Summit in December of 2022 of $15 billion in business investments, the west is scrambling to catch up to China in Africa. At the same time, western nations writ large are struggling to overcome the stigma of colonialism on the continent (Cohen 2022).

While the EU and other western institutions have a tendency to invoke normative principles toward African development by bridging foreign aid packages with the development of human and social initiatives, the raw reality of the decisions made in

African investments sometimes actually contradict the EU's normative rhetoric (Bountagkidis, Fragkos, Frangos 2015, p. 107). This might mean that such rhetoric serves more as a domestic messaging backdrop for more pragmatic and economically advantageous initiatives in Africa. This presents a potentially dangerous situation if there is proven to be a dissonance between rhetoric and action. Europeans may become disillusioned by the lack of follow-through, despite the potential for real-world gains associated with a more realist model of engagement and investment.

Russia

Russia also poses significant challenges for Western European engagements in Africa. This became especially apparent in the mid-2010s with a "Resurgent Russia" conducting operations in support of its interest in the Middle East (Syria), Europe (Crimea and Eastern Ukraine), and Africa. Russian paramilitary presence in Africa first manifested in 2017 in Sudan, but their activities spread as far as the Central African Republic, Madagascar, Libya, and Mozambique (Smith 2022, p. 5). Since that time, they have established a significant presence in the Sahel.

Wagner group's success in striking a deal with the Malian regime to control Mali's state-owned gold mines in exchange for armed fighters is just one such example of the dynamic at play in the Sahel (Smith 2022, p. 7). Europeans, in order to even maintain a foothold in Africa, will have to decide if they will continue their tradition of supporting initiatives with normative rhetoric. One such example of this dynamic is the French Ministry of Armed Forces statement criticizing CAR authorities on their decision to work with the non-state actor Wagner Group (Cohen 2022). European countries may eventually need to consider pivoting to a more pragmatic, less ideological approach to engagement in Africa in light of the competition posed by authoritarian states whose consciences are less burdened.

One major concern for Europeans' future in Africa lies in the control of propaganda and narrative. For example, Russian masters of propaganda, Wagner founder Evgeny Prigozhin and his close collaborator Alexander Ivanov, have stated that the regime change in Burkina Faso was "yet another milestone in a new era of decolonization". Their further suggestion that Wagner instructors train the new regime's armed forces illustrate how control of the narrative shapes the environment (Smith 2022, p. 6).

Russian propaganda is transmitted through popular radio wherever Russians maintain a presence (Cohen 2022). It logically follows that: 1) if you are not on the ground, you have no narrative, and 2) if you control the narrative, you can influence or even control the local leadership and population.

Clearly, Russia's understanding of the application of raw power versus the hard-earned establishment of stable accountable leadership in African governments grants them an edge in the competition for Africa (Smith 2022, p. 9). As demonstrated by 20 years of attempts in Afghanistan, the nation-building approach can be overly challenging and demoralizing.

The Unites States

The United States has also involved itself in the competition for resources in Africa. It was predicted that in the coming decades, it will import more oil from Africa than the entire Middle East (Kotsopoulos 2007). The U.S. is also interested in maintaining a more robust military presence in Africa. In 2007, the U.S. Africa Command (USAFRICOM) headquarters for the region was established (Kotsopoulos 2007). This is significant in that the U.S. is a western, democratic ally who generally shares Europe's neo-liberal ideologies, has strong military ties with NATO, and is also a valuable trading partner. This would indicate that the U.S. and EU should be natural partners in African engagement. But the U.S. is also a competitor when it comes to limited resources – especially oil and gas.

Human rights and Democracy

The EU touts itself as a force for good, and it applies normative neo-liberal ideologies of cooperation in the promotion of human rights and democracy when designing its policies. As was previously mentioned, priorities proposed for the EU-Africa partnership include "consolidating democracy and good governance" and "reaching human development standards" (Forysiński, Emmanuel 2020, p. 69).

The African continent has many difficulties, including a large number (36) of the world's most vulnerable countries, which harbour governance issues, civil conflicts, house 390 million people living in poverty, and last but not least, bear the brunt of the effects of

global climate change (Forysiński, Emmanuel 2020, p. 70). EU engagement will need to target all these difficulties if it expects to see any results.

Autocratic and populist rule in Africa remains a force to be reckoned with. It was unable to be overcome through the French mission there (Smith 2022, p. 9), and it is unlikely to disappear anytime soon. Thus, it is vitally important for Europe that democratic reforms in North Africa are pursued. Europeans will have new economic opportunities and significant strategic opportunities to address the enduring issues of migration and radicalization, pursue regional problem-solving, expand European influence throughout the Middle East, and forge closer ties with the larger Islamic and Arab worlds if more open and dynamic societies can establish themselves in a region that has long been seen as a threat (Witney, Dworkin 2012, p. 5).

As former United Nations Secretary-General Kofi Annan once stated: “We will not enjoy development without security, we will not enjoy security without development, and we will not enjoy either without respect for human rights” (Kotsopoulos 2007).

Conclusion

Europe is burdened by its historical treatment of Africa and must acknowledge and overcome that stigma in order to move forward. EU actions and rhetoric must be aligned. Africa is emerging as a battleground for strategic competition. Authoritarianism seems to have the advantage in the current environment. Neo-liberal ideology and “soft power” will require more effort to employ. Ultimately, alignment between ideology, actions and narrative will be required in order find success.

African Security Situation: Instability and Migration

The security situation across Africa not only threatens the stability for those on the continent, but that of Europeans at home as well. Here I break down the potential negative results of the security situation into constituent parts: instability and migration. I will examine each of them in terms of their effect on European and African nations, and how this potentially shapes motivations for EU engagement and cooperation with Africa. This arena is where the nexus between security and development lies. As stated in the European Security Strategy from 2009, “There cannot be sustainable

development without peace and security, and without development and poverty eradication there will be no sustainable peace" (Council of the European Union. General Secretariat of the Council. 2009, p. 19).

It is necessary to note that countering terrorism abroad to protect oneself has previously been used to justify European activities in Africa. France's intervention in Mali (a former French colony) in 2013, for example, was specifically intended to prevent a takeover by jihadi forces (Smith 2022, p. 2). The counterterrorism argument for France's military presence in Africa falls somewhat flat when one considers that none of the numerous terrorist attacks within France have been traced to the Sahel (Smith 2022, p. 8). Henceforth, the terrorism discussion will be absent from this paper.

Instability

Instability threatens local and regional security, and ultimately precipitates key threats of regional conflicts, organised crime, and state failure (ESS, p. 30-32). Therefore, in order to eliminate such negative symptoms, the stability of the state and local governments lies at the heart of the problem. Supporting lawful governments, and mediating regional conflicts is essential in achieving stability.

In 2010, U.S. Secretary of Defence Robert Gates identified so-called weak states as "the main security challenge of our time". He argued for the necessity of providing them with the equipment, training and other security assistance (Karlin 2017, p. 111). If he is correct, then a strong security assistance program to include training and equipment support would be a noble initiative in fostering regional security.

Conversely, a classic example of a failed security assistance initiative is the United States' attempts to help Mali strengthen its own military forces, which backfired when a U.S.-trained officer of the Malian armed forces staged a coup in 2012 (Karlin 2017, p. 113). This highlights the dangers of unintended consequences hidden in the provision of security assistance to a government that does not necessarily share the values of the provider.

In fact, sub-Saharan Africa has experienced increased insecurity in 2021/2022, to include a significant number of attempted and successful coups (Sub-Saharan Africa

2022, p. 223). This means that European initiatives must carefully and completely assess the risks associated with security assistance to Africa before committing to any endeavour.

Another contributor to instability is border and resource disputes between regional powers. One such example is Northern Africa. The possibility of confrontation between Algeria and Morocco is now more plausible than it has been in recent years due to this radically altering regional dynamic (Middle East and North Africa 2022, p. 296). These kinds of sour relationships foster consternation with respect to energy security, human rights, and migration.

Migration

Migration – specifically “mass migration” – is a major area of concern for the EU. Such flows substantially are a result of instability in the Sahel. Coups in Mali and Burkina Faso have escalated this concern even more (Sub-Saharan Africa 2022, p. 327).

Algeria currently hosts some 173,000 refugees from the Western Sahara region (Middle East and North Africa 2022, p. 288), and given that there are already 2.6 million internally displaced persons in the Sahel, according to the UN High Commissioner for Refugees, European governments are naturally fearful of a replay of the refugee and migration crises of 2014–15 (Sub-Saharan Africa 2022, p. 328).

The announcement by French President Emmanuel Macron about the planned withdrawal of French and European troops from Mali and ending the counter-insurgency mission Operation Barkhane is expected to further weaken the security situation in northern Mali, and consequently intensify the migration flow (Sub-Saharan Africa 2022, p. 328).

If EU members truly wish to avoid repeats of the migrant crisis of 2014, then engagement in Africa to promote the stability of the governments there is imperative. Promoting and supporting stable governments to improve regional security is key to reducing instability, countering terrorist groups, and reducing migrations. The unfortunate reality, however, is that existing governments may not fall into the category of “desirable partners”, either because they are autocratic leaders clinging to power at

all costs, or egregious violators of human rights, or both. This reality will have to be managed, and risks mitigated, if there is any hope of arriving at (or at least making progress towards) that elusive nexus between development and security.

Conclusion

Regional security is inextricably linked to regional stability. Instability in Africa leads to poverty and mass migrations, which can threaten the stability and security in Europe. Security and development go hand in hand, they exist in balance, and we cannot have one without the other. Therefore, a multi-pronged approach to development, security, and the promotion of human rights is necessary.

Conclusions

In this paper, I began by providing a background discussion of the relationship between Europe and Africa throughout the past 2 centuries and have laid out the current state of play between the two continents. In short, Europe is continuing its trajectory towards partnership and cooperation in Africa.

In the analysis, I first explained the value of economic potential for EU-Africa partnerships by examining the risks and opportunities with respect to resources and energy, and with respect to markets and trade. Europe cannot afford to ignore African resources and markets simply because of the challenges Africa presents.

I then discussed the importance of strategic competition by outlining the history of such competition in the form of colonialism, and how Europe's colonial history is at odds with 21st century ideology. I also described the interests of other strategic competitors, and the challenges posed by conflicting ideologies and goals. Then, I Described how the narrative is so crucial in this competition.

Finally, I considered the African security situation and its constituent components of instability and migration. I explained why political and social instability on the African continent are of great concern for Europe. I discussed how mass migration has affected and could continue to affect European stability. And I discussed the reciprocal roles that development and security play in this environment.

My aim in this paper was to explore the question of why does the European Union continues to engage in Africa despite the costs and setbacks, and how might resources and effort be better applied to produce a favourable outcome. In other words, I have explored the question: Is EU engagement an Africa a thankless task or a necessary endeavour? The conclusions in each chapter reveal that the cost of not engaging in Africa through all possible instruments of national power can lead the EU to a worsening situation. To improve its energy security, explore new resources cooperatively, remain a global competitor, maintain security, and continue to broadcast its values of democracy and human rights, Europe must continue to foster relationships in Africa.

So, what courses of action might Europe pursue?

1) Acknowledge the negative aspects of its colonial history without allowing those sensitivities to hamper opportunities.
2) Foster positive relationships with North African neighbours across the Mediterranean, as well as the relationships between them to promote regional peace and stability and ensure energy trade remains open.
3) Acknowledge the advantages that strategic competitors such as China and Russia possess given the current power landscape in sub-Saharan Africa and design a strategy that enables favourable conditions for the EU-AU vision despite the competition.
4) Continue to engage in security assistance endeavours, but with careful attention to negative unintended outcomes such as military coups, or extremist takeovers to promote stability, alleviate poverty, and reduce the likelihood of mass migration northward.
5) More aggressively pursue trade partnership opportunities with North African nations to improve economic cooperation in the region.
6) Continue to promote European values of human rights, freedom, and democracy as a force for good, and a positive step toward the security-development nexus, but with the understanding that African leaders and populations may not be ready to immediately receive them.

This may mean that Europe, without necessarily compromising its values, should be honest and pragmatic about its complicity when dealing with autocratic leaders of African nations, and its decisions on allocation of foreign aid, to remain engaged and to work toward a future with Africa that is equitable, respectful, and fosters prosperity that is mutually beneficial.

Bibliography

ADEBAJO, Adekeye and WHITEMAN, Kaye (eds.), 2012. The EU and Africa: From Eurafrique to Afro-Europa. paperback original. C. Hurst & Co. (Publishers) Ltd., 41 Great Russel Street, London, WC1B 3PL. ISBN 978-1-84904-171-3.

BOUNTAGKIDIS, Georgios, FRAGKOS, Konstantinos and FRANGOS, Christos, 2015. EU Development Aid towards Sub-Saharan Africa: Exploring the Normative Principle. Social Sciences. 9 January 2015. Vol. 4, no. 1, p. 85–116. DOI 10.3390/socsci4010085.

BROOKES, Peter, 2007. Into Africa: China's Grab for Influence and Oil. Heritage Lectures. 26 March 2007. No. 1006.

COHEN, Roger, 2022. Putin Wants Fealty, and He's Found it in Africa. New York Times. Online. 24 December 2022. [Accessed 26 February 2023]. Available from: https://www.nytimes.com/2022/12/24/world/africa/central-african-republic-russia-wagner.html.

COUNCIL OF THE EUROPEAN UNION. GENERAL SECRETARIAT OF THE COUNCIL, 2009. European Security Strategy: a secure Europe in a better world. Online. LU: Publications Office. [Accessed 27 February 2023]. Available from: https://data.europa.eu/doi/10.2860/1402.

FORYSIŃSKI, Wojciech and EMMANUEL, Achiri, 2020. EU-Africa Relations: Towards a New Comprehensive Strategy With Africa. Between a Rock and a Hard Place. Przegląd Strategiczny ("Strategic Review"). 31 December 2020. No. 13, p. 61–78. DOI 10.14746/ps.2020.1.4.

FOSTER, Vivien, BUTTERFIELD, William and CHEN, Chuan, 2009. Building Bridges: China's Growing Role as Infrastructure Financier for Africa. Online. The World Bank. [Accessed 21 February 2023]. ISBN 978-0-8213-7554-9.

GERBER, Leon, 2012. Africa and the EU mineral trade. Polinares: EU Policy on Natural Resources. 2012. Vol. D5, no. 1, p. 1–12.

KARLIN, Mara, 2017. Why Military Assistance Programs Disappoint. Foreign Affairs. December 2017. Vol. 96, no. 6.

KOTSOPOULOS, John, 2007. The EU and Africa: coming together at last? July 2007. European Policy Centre.

Middle East and North Africa, 2022. Strategic Survey. Vol. 122, no. 1, p. 275–318. DOI 10.1080/04597230.2022.2145094.

SMITH, Stephen, 2022. Macron's Mess in the Sahel How a Failed French Mission Gave Russia New Sway in Africa. Foreign Affairs. Online. 10 March 2022. [Accessed 26 February 2023]. Available from: https://www.foreignaffairs.com/west-africa/macrons-mess-sahel.

Sub-Saharan Africa, 2022. Strategic Survey. Vol. 122, no. 1, p. 319–358. DOI 10.1080/04597230.2022.2145095.

Threat-based defence planning: implications for Canada, 2021. Online. Network for Strategic Analysis. [Accessed 26 February 2023]. Available from: https://ras-nsa.ca/wp-content/uploads/2021/03/Report-on-CJOC-Defence-Planning-Project.pdf.

WEBSTER, Richard A., MAGDOFF, Harry and NOWELL, Charles E., 2022. Western colonialism - Partition of Africa | Britannica. Online. 13 November 2022. [Accessed 26 February 2023]. Available from: https://www.britannica.com/topic/Western-colonialism/Partition-of-Africa.

WITNEY, Nick and DWORKIN, Anthony, 2012. A power audit of EU-North Africa relations. London: European Council on Foreign Relations. ISBN 978-1-906538-62-0.

MAJ Nerijus LAUGALYS. The role of cyber attacks in Russia's military operations in Georgia and Ukraine

Introduction

Throughout history, nations strived to incorporate new technological advancements into military operations to gain an advantage over their opponents. For example, five years after inventing the aeroplane, the Wright brothers began producing aircraft for the United States military, which was employed in joint operations with the infantry during World War I (Even, Siman-Tov, 2012). Aircraft introduced the aerial domain to the military theatre, forcing nations to adapt their strategies and doctrines to take advantage of new technology. Furthermore, during World War II, the German *Blitzkrieg* tactics successfully integrated tanks and aircraft into manoeuvre warfare, demonstrating their ability to achieve superiority over the enemy despite possessing comparable technology (Goldman, Arquilla, 2014). Although global powers had access to technological advancements, those who applied them most efficiently had the best outcome.

The 21st century introduced a cyber domain to the battlefield, influencing national strategies and doctrines. Russia acknowledged the US-led coalition's effective integration of information technology advancements during the 1991 Gulf War (Lambeth, 1992). Similarly, Russia recognised the importance of information operations in its military campaigns. During the 1999 Chechen War, Kremlin could control the traditional news environment but struggled to prevent Chechens from successfully communicating information about their brave fight through the Internet (Even, Siman-Tov, 2012). Later, Russia demonstrated that cyberattacks are part of its toolbox for seeking strategic objectives. In 2007, Russia launched the first known cyber campaign against a state in Estonia, and the following year, it combined cyberattacks with kinetic military actions in Georgia (Even, Siman-Tov, 2012). Next, Russia's conflicts in Ukraine in 2014 (Hakala, Melnychuk, 2021) and the large-scale invasion in 2022 have been supported by cyberattacks on the Ukrainian government, infrastructure and economic institutions (Microsoft, 2022). Russia's increased use of cyberattacks raises the question of whether it has mastered the employment of cyber technology to gain an advantage over its opponents and what the true role of cyberattacks is in Russia's military campaigns.

This paper aims to analyse how Russia employs cyberattacks to shape military battlefield for conventional operations and identify how cyberattacks support the main objectives of warfare. The essay is divided into two major sections. The first part will examine the role of cyber in Russia's doctrine documents and cyber adaptation in Russian operational art via force, space and time operational factors. The second section will provide a comparative analysis of how cyberattacks were utilised and balanced through force, space and time operational factors in recent military conflicts in Georgia (2008), Ukraine (2014), and Ukraine (2022).

Cyber Role in Russia's Doctrine

Russia's cyberspace perception is different from Western countries. Firstly, the foundations of Russia's cyber adaptation roots in its history. According to scholars, Russia's cyber approach to contemporary military operations was formed over a century ago (Lilly, Cheravitch, 2020). For instance, the Czarist Secret Service Okhrana initiated deception against revolutionary groups in late 1860 (Ward, 2014), and Czar established the Maskirovka School in 1904, which offered foundations employed today (Thomas, 2004). Later Soviet ideologies also influenced Russia's cyber adoption. Researchers claim that ideologies from the Soviet-era, such as 'reflexive control', 'active measures', and 'maskirovka', influenced Russian cyber capabilities integration (Hakala, Melnychuk, 2021). These concepts aim to gain information superiority over opponents (Hakala, Melnychuk, 2021). Thus, Russia's historical background significantly influenced cyber adaptation with the primary goal of achieving information superiority over adversaries.

Cyber in Russian doctrines is not mentioned as a separate function or domain and is represented as a component of information warfare. Looking chronologically, Russia in military doctrine (2000) introduced the need for its troops to act in the *'information space*' and counter '*information threats',* emphasising psychological effects (Darczewska, 2016). Thus, Russia may have identified the need for new capabilities in its military after the last activities in the Chechen war (1999), when it struggled to achieve online information dominance. These capabilities were tied to information space rather than cyberspace. Furthermore, Russia emphasised the need to develop defensive measures against foreign technical activities and their psychological impact

in the Information Security Doctrine (2000) (Darczewska, 2016), where information was identified as a weapon (Bagge, 2019). Although Russia has identified security threats from foreign countries, it likely planned to adopt technology against opponents from the same perspective. In 2000, Russia recognised the need for new information-related capabilities in military operations, emphasising information as a weapon and its psychological effects.

In 2010, Russian doctrines intensified information warfare's significance and introduced the importance of non-military means. Academics suggest that Russian military doctrine (2010) emphasised information warfare and its tools before using military power to shape the environment and achieve political goals (Bagge, 2019). Information warfare technologies like cyberattacks could support strategic objectives and shape the battlefield. Moreover, this doctrine focuses on information warfare to achieve strategic goals without conventional force or to influence a favourable reaction from the international community for military force employment (RF, 2010). Therefore, Russia might use its cyber capabilities as an information warfare component to achieve political goals or to shape the battlefield for force deployment.

Furthermore, cyber is integrated into Russian military information warfare doctrine. Giles (2012) states that the 2011 Russian publication 'Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in Information Space' could be seen as a Russian cyber doctrine outlining the role of the Russian military in cyberspace. It describes the main information-space definitions, principles and rules (Long, 2013). Like other publications, it emphasised cyber as an information warfare component and its psychological effects. Additionally, it more narrowly describes the military actions in cyberspace, including 'sphere of intelligence, operational deception, radioelectronic combat, communications, covert and automated command and control' (Long, 2013). Furthermore, it describes the communication systems' vulnerability, cross-border effects, and speed (Long, 2013). This doctrine reveals that cyber capabilities were integrated into Russian military functions for intelligence gathering and gaining advantage through covert cyber activities as part of information warfare.

Moreover, Russian general Gerasimov's (2016) publication 'The Value of Science Is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Conducting Combat Operation' emphasises the significance of non-military means to

neutralise opponents' capabilities in contemporary conflicts. First, Gerasimov recognised that information space had opened new avenues for technologically degrading the opponent's fighting potential and exploiting enemy vulnerabilities (Galeotti, 2014). Second, Gerasimov acknowledged the significance of close coordination between military intelligence and information operations (Galeotti, 2014). As identified, Russia's information operations may include planning, coordinating, and executing cyberattacks across several Russian agencies. Third, Gerasimov's article introduced the offensive cyber role, enabling peacetime covert operations without attributing the military or Russian government (Medvedev, 2015). To summarise Gerasimov's ideas, cyberattacks can be used as an offensive tool in close collaboration with different agencies during peacetime to neutralise Russian opponents' capabilities.

In summary, Russia views the cyberattacks role differently than Western nations. Cyberattacks support Russian information warfare and have psychological effects. Additionally, they have incorporated cyberattacks into their military to gain an advantage through coordinated operations to reduce their opponents' fighting capabilities. Russia also recognises cyberattacks' benefits, which could be used to shape the battlefield across the border during peacetime to weaken their opponent before a conventional attack.

Cyber Role in Russia's operational art

To comprehend the impact of Russia's cyberattacks on the military battlefield, it is important to examine how Russian strategists view the incorporation of cyberattacks into operational art. In contrast to the land, sea, and air domains, the cyber domain is relatively new. It lacks well-developed operational art theory and analysis, not just in Russia but also in Western countries. Therefore, this chapter examines how Russia views cyberattack employment vis-a-vis operational factors, such as force, space and time.

Cyber application in operational art is crucial in achieving strategic and operational objectives. According to Vego (2009), operational art links tactical operations to strategic objectives and synchronises all military and non-military power sources to achieve operational goals. The operational art value may be overlooked by depending

too heavily on technological advancement. Moreover, technology cannot replace operational art but must be adapted to new capabilities (Vego, 2009). Thus, cyberattacks cannot efficiently support strategic objectives without adaptation of the operational art.

Russian cyberattacks capacity and efficiency highly depend on cyber force combat potential. According to Vego (2009), force defines power and capacity to use military and non-military means. Therefore, Russian cyber troops analysis is necessary to comprehend its capabilities, *modus operandi*, strengths and weaknesses.

Russian cyber organisational structure is large and has vast cyber capabilities. As depicted in Figure 1, Russia has three key cyber actors: the Federal Security Service (FSB), the Main Intelligence Directorate (GRU), and the Foreign Intelligence Service (SVR). FSB is a former Committee for State Security (KGB) institution focusing on domestic intelligence and maintaining a dominant role amongst Russian cyber actors (Soldatov, Borogan, 2021). FSB has two main cyber directorates, the 18th and 16^{th,} focusing on computer network exploitation (CNE), cybercrime and espionage operations (Pingios, 2021). Next, SVR is the former KGB spy agency focusing on foreign intelligence (Soldatov, Borogan, 2021). GRU's 8th and 6th directorates oversee and conduct military cyber operations, respectively (Soldatov, Borogan, 2021). Although these organisations have their functions and areas of responsibility, sometimes they act oppositely. For instance, SVR and GRU attack domestic cyber targets, while FSB international ones (Soldatov, Borogan, 2021). The Russian cyber force comprises former Soviet organisations that have developed CNE, attack, and espionage capabilities that could be utilised on the military battlefield. As a military unit, the GRU plays a significant role in cyberattack employment on the battlefield; however, SVR and FSB could also be involved as their areas of operation overlap.

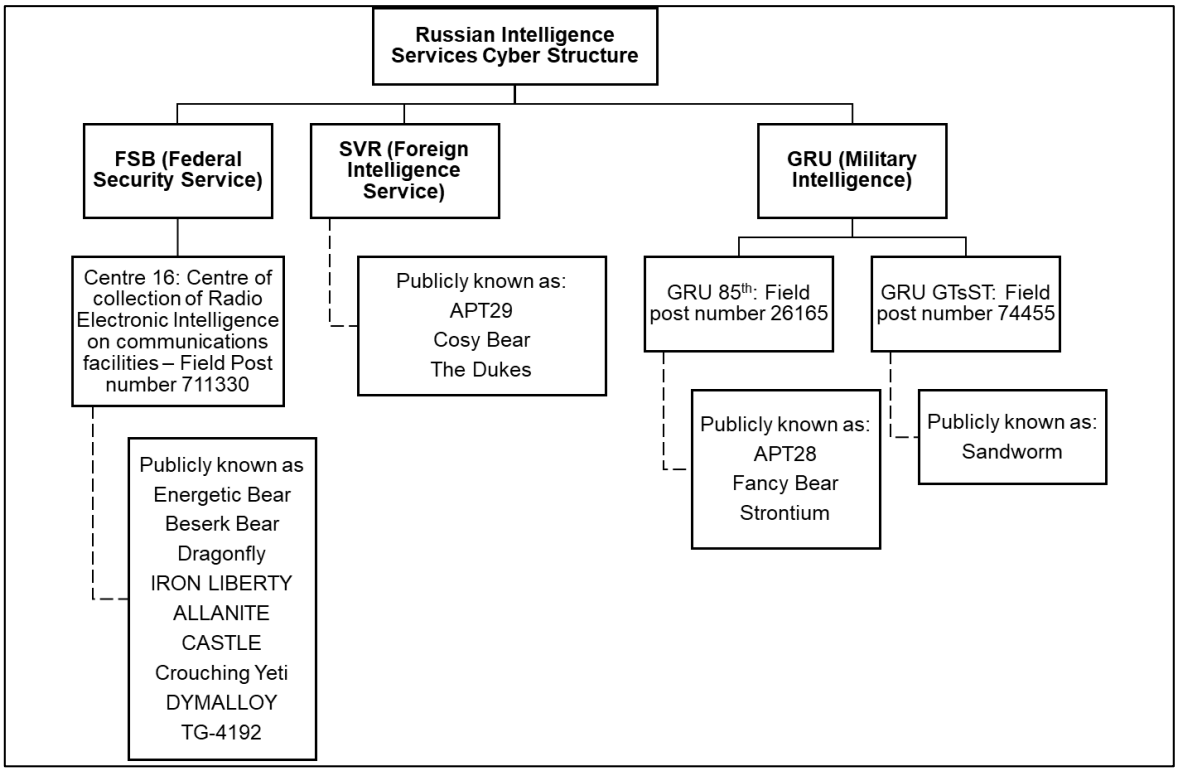


Figure 1. Russian Intelligence Services Cyber Structure. Source: (GOV.UK, 2022)

Russian cyber force combat potential highly depends on private and criminal sectors. Sophisticated cyberspace technology development requires advanced research and highly skilled technicians. In 2009, *'information security'* was added to the curriculum at 73 Russian universities (Soldatov, Borogan, 2021). Thus, Russia has promoted cyber education nationally to gain an advantage over adversaries. Furthermore, Russia heavily relies on the private sector. Researchers claim FSB connections with cybersecurity companies such as Kaspersky Lab for information sharing, recruitment and training (Soldatov, Borogan, 2021). Additionally, due to their anonymity and ease of mobilisation, Russian cyber institutions cooperate with hacktivists, cybercriminals, and so-called 'patriotic' hackers (Connell, Vogler, 2016). However, collaboration with criminals poses additional challenges to the effectiveness of Russia's cyber force. According to experts, Russian criminal organisations have collaborated with and opposed the government (Levi, 2022). These results indicate that Russia is utilising all its available resources to achieve its objectives; however, it presents additional challenges and constraints for Russian cyber efficacy.

Russia's cyber organisational structure is not only large but also complex. First, Russia lacks a centralised Cyber Command, and there is no clear operational reporting and accountability mechanism, which reduces its cyber operational efficacy (Soldatov,

Borogan, 2021). In comparison, western countries have well-defined Cyber Command structures to ensure centralised planning and unity of command and effort tailoring resources to strategic and operational objectives. Second, effective cooperation is hindered by using post-Soviet methods to compel cybergroups and hackers to participate in cyber campaigns. For instance, civilian organisations and hackers are frequently coerced or solicited to contribute to cyber operations (Cheravitch, Lilly, 2020), which reduces collaboration effectiveness. As a result, the lack of Cyber Command and Russia's legacy culture impedes successful collaboration among internal and external cyber actors.

Space operational factor provides vast opportunities for cyberattack employment. Cyberspace is distinct from the land, sea, and air domains, featuring undefined size and boundaries, global distance, and artificial infrastructure, which creates conditions for unconventional warfare (Hall, 2011). Cyberspace global interconnectivity provides opportunities to conduct cyberattacks across borders without or before deploying actual troops. Furthermore, Russian military thinkers Chibisov and Vodkin suggested that '*information strikes'*, including cyberattacks, could be employed operationally 'over 300–400 km along the front and up to 450–500 km in depth' and strategically along the entire theatre (Kofman et al., 2021). Cyberattacks and operational distances linkage suggests their combination with long-range fire systems on the operational level. According to researchers, Russia ties its new technology capabilities to classical offensive operational art, where electronic means were employed to disorganise the enemy on the battlefield (Kofman et al., 2021). Thus, cyber provides long-range offensive capabilities. Operationally, Russia likely combines cyberattacks with their long-range firing weapons; however, strategically, it intends to utilise them throughout the entire theatre.

Time factor needs special consideration for cyberattack operational employment. Due to internet speed, it may be mistakenly thought that cyberattacks can be executed rapidly, but in reality, the process is more complex and time-consuming. Cybersecurity company PaloAlto (2022) defines six cyberattack's lifecycle stages: 'reconnaissance, weaponization and delivery, exploitation, installation, command and control, and actions on the objective'. Failure at any stage could prevent the attack from achieving its objective (PaloAlto, 2022). Consequently, planning and preparation consume most of a cyberattack's lifecycle. Furthermore, Russia is considering synchronising

cyberattacks with other military domains in a single geographic area (Hall, 2011). Nonetheless, cyberattack integration and synchronisation with joint operations can be challenging due to the complexity of cyberattacks and the time required to exploit adversary vulnerabilities. Therefore, cyberattack utilization during peacetime provides more time for planning and crafting specific attack scenarios without the pressure of a wartime situation. Overall, cyberattacks' complexity and time needed for preparation make their operational utilisation more favourable during peacetime and in the initial war phase.

Analysis of operational factors suggests Russia is incorporating cyberattacks into its operational art. The country's cyber force comprises FSB, SVR, and GRU, which have significant capabilities and receive support from cybercriminals and hacktivists. However, the absence of centralised command and post-Soviet organisational culture hinders cooperation and combat effectiveness. Additionally, Russian strategists see the potential to use cyberattacks during peacetime and conventionally combine them with long-range firing systems. Planning and preparation for cyberattacks are time-consuming, making them less advantageous in dynamic conventional warfare. Analysing Russia's recent conflicts can help us better understand their use of cyberattacks.

Comparative analysis

Georgia 2008

The 2008 Russo-Georgian war signalled the new cyber-era beginning in conventional warfare. Russia first time, used cyberattacks as a force multiplier for kinetic operations (Mazanec, 2015). Analysing cyberattacks' balance within operational factors to achieve strategic objectives in this war helps to assess Russia's initial conventional cyber capacities.

Russia launched cyberattacks against Georgia to gain information dominance and destabilise the country's government and economy. Initially, Russia targeted Georgian media and government websites utilising Distributed Denial of Service (DDoS) and web-defacement attacks (Kozlowski, 2014). Merriam-Webster dictionary (1998) DDoS attack defines as 'an attempt to interfere with the normal operations of an online service

(such as a website or application) by overwhelming it with repeated automated requests for data from multiple sources'. DDoS attacks can have immediate impacts by denying targeted servers or services. In the second stage, more sophisticated Structured Query Language injection attacks were launched against financial and educational organisations (Kozlowski, 2014). This attack can provide hackers access to databases containing confidential login credentials, financial records, and all website content (Shakarian, 2011). According to this phasing, Russia has prioritised its objectives and aimed towards them at various times. Russian hackers shut down the Georgian central commercial bank for ten days while comparing Georgian President Saakashvili to Adolf Hitler on governmental websites (Shakarian, 2011). Experts suggest that Russia aimed to disrupt the Georgian government and civilian operations and impede the international dissemination of information about the conflict (Shakarian, 2011). These findings indicate that in 2008, Russia used cyberattacks to gain information superiority by destabilising the Georgian government and economy and preventing the dissemination of conflict-related information to the international community.

Analysis of balancing cyberattacks with operational factors can help assess how Russian objectives were aimed to achieve. The time factor was significant in this war. First, several months before conventional operations, the first cyberattacks were launched. In July, security companies identified DDoS attacks and flooding message 'win+love+in+Russia' on Georgian servers (Kozlowski, 2014). It suggests that Russia began shaping the battlefield two months before the conventional operation to intimidate Georgia and test its cyber capabilities. Second, Russia has incorporated cyberattacks into its operational planning, with distinct targets in two stages. Third, Russia manipulated Georgian Internet communications via DDoS attacks, creating a cyber blockade (Medvedev, 2015). DDoS attacks require less preparation time but typically have a shorter impact than more complex tailored cyberattacks. For instance, despite pro-Russian hackers blocking Georgia's official websites, Georgians recreated them on more secure foreign servers (Medvedev, 2015), thus countering such attacks. Time operational factor analysis suggests that Russia had been planning and testing cyberattacks for several months before the invasion of Georgia. Additionally, it used less sophisticated attacks aiming to overwhelm and create a cyber blockade but were

temporarily effective due to Georgian security experts' response and international support.

Next, the operational space factor was also important in cyberattack employment. In 2008, Georgian internet infrastructure was connected to the international world through Russia, Turkey, Armenia and Azerbaijan landlines (Shakarian, 2011). Landlines in Georgia can be considered key terrain in cyberspace, providing the state's main connection points to the international world. Experts claim that Russia has used DDoS attacks against bottleneck points to deny or redirect internet traffic (Medvedev, 2015). Additionally, cyberattacks successfully shut down cell phone systems, disrupting governmental and civilian communications domestically and internationally (Shakarian, 2011). Consequently, Russia conducted cyberattacks on Georgian information infrastructure, exploiting vulnerable areas to disrupt domestic and international communication.

Furthermore, the Russian cyber force operational factor heavily relied on criminal groups. Experts link the majority of cyberattacks to the Russian criminal group Russian Business Network, which is believed to have ties to the Kremlin (Shakarian, 2011). Criminals' employment provided Russia with several benefits. It gave Russia plausible deniability and access to additional resources and expertise.

Additionally, Russia employed 'patriotic' hacktivists to enhance its cyber power against Georgia. After Russian troops crossed the Georgian border, Russia launched the StopGeorgia.ru website with detailed cyberattack instructions (Hakala, Melnychuk, 2021). This allowed Russia to achieve an overwhelming effect against Georgia. Moreover, media and internet infrastructure were not attacked conventionally (Shakarian, 2011). These facts indicate that Russia has coordinated and divided kinetic and non-kinetic targeting. In conclusion, criminal organisations and hacktivists targeting media and internet objects reinforced Russia's combat potential during the war.

However, cyberattacks had to be coordinated by Russian institutions. Greenberg (2019) claimed FSB was the primary coordinator of cyberattacks, with GRU taking a back seat. The FSB's connections with cybersecurity firms and cybercriminals likely enabled them to effectively organise these attacks, positioning them as the main coordinating force.

Analysis of the Russo-Georgian War suggests that the main objective of cyberattacks was to gain information superiority, disorganise Georgian political, economic and media systems, and create favourable conditions for conventional forces' actions. However, cyberattacks had limited effects due to international support. Operational analysis revealed that Russia shaped the battlefield, tested cyberattacks several months before the invasion, and intensified them during the conventional attack. Space factor analysis depicts that Russia was aware of Georgian cyberspace infrastructure and exploited its vulnerabilities to gain an advantage from cyberattacks. Moreover, Russian criminal organisations and 'patriotic' hacktivists enabled Russia to deny its cyberattack involvement. Although Russia didn't get the full potential from cyberattacks, its operational art benefited from the knowledge and lessons gained for future military campaigns.

Ukraine 2014

In 2014, Russia launched a hybrid warfare campaign against Ukraine with the main objective of annexing Crimea. Russia employed comprehensive coordination of military, economic, diplomatic, political, information and other activities to achieve strategic goals (Walker, 2015). Cyberattacks, as an important hybrid warfare component, have been an integral part of this effort.

First, Russia used a coordinated cyber campaign and information tools to disrupt Ukraine's communication and operations, creating confusion and uncertainty (Connell, Vogler, 2016). Secondly, Russia employed cyberattacks to disseminate propaganda, fake news, and misinformation. Russia aimed to discredit the Ukrainian government and create a narrative which portrayed Crimea's annexation as legitimised (Connell, Vogler, 2016). However, instead of cyberattacks, kinetic actions were sometimes used to disrupt communications during the Crimea seizure. For instance, personnel without uniforms attacked Ukrtelecom infrastructure, disrupting landlines and cell phones and blocking information exchange between Crimea and Kyiv (Bagge, 2019). Consequently, Ukraine's decision-makers access to information and situational awareness was disrupted, hindering their ability to coordinate during the national security crisis. Cyberattacks combined with kinetic actions demonstrated hybrid warfare effectiveness in undermining Ukrainian government operations.

From a time perspective, first cyberattacks started before kinetic actions. During the Euromaidan protests, hacker groups already conducted DDoS and other cyberattacks and used information leaks for propaganda (Stinissen, 2015). It demonstrates that Russia uses non-military cyber activities before kinetic actions. Furthermore, Russia has intensified cyberattacks during military operations in Crimea (Stinissen, 2015). Accordingly, Russia was planning and synchronising cyber efforts with kinetic actions. Moreover, Russia conducted DDoS and website defacement cyberattacks against Ukraine's mobile infrastructure, parliament members' phones and security communications (Stinissen, 2015). Hence, Russia deployed cyberattacks for rapid information superiority. Time analysis suggests that Russia in Crimea employed cyberattacks before military actions, coordinated them with conventional activities, and employed less sophisticated attacks to gain swift information superiority.

Cyberspace employment in the Crimea operation reveals a modified approach to Russia's cyber operational art. Russia had similar cyber targets in Ukraine as in Georgia. For instance, Russian hackers targeted government institutions and communication systems (Medvedev, 2015). Accordingly, Russia aimed to gain rapid information superiority. However, the cyberattacks scope in this operation was significantly greater. Russia has expanded the targets list, including NATO allies. CyberBerkut, a pro-Russian organisation, has claimed responsibility for DDoS attacks against NATO websites, including the NATO Cooperative Cyber Defence Centre of Excellence in Estonia and unclassified NATO email (Jasper, 2020). It suggests that Russia used cyberattacks to influence global support for Ukraine. Russia also demonstrated more advanced cyber capabilities when targeting Ukraine's presidential elections. CyberBerkut disrupted the Central Electoral Commission's critical infrastructure and electoral system components during the election (Jasper, 2020). Cyberspace targets analysis demonstrates that Russia attacked governmental institutions and communication infrastructure as previously. However, it expanded its cyber activities internationally and deployed more sophisticated cyberattacks.

Russian cyber force employment in Ukraine was similar to the previous conflict yet introduced new methods. Similarly, Russia increasingly utilised non-state cyber actors (Stinissen, 2015). It ensured Russia's cyberattacks' plausible deniability. However, instead of Russian patriotic hackers, Russia relied on the Ukrainian-based, pro-Russian hacking group CyberBerkut, which claimed to operate from Ukraine

(Medvedev, 2015). Ukrainian proxy groups' employment benefited hybrid warfare plan disguising Russian involvement. According to Ukraine researchers, FSB controls CyberBerkut, or it is an FSB unit (Kostyuk, Zhukov, 2019). However, scholars Lilly and Cheravitch (2020) argue that the Russian conflict in Ukraine empowered GRU to lead cyber offensive operations. Additionally, political scholar Galeotti (2014) claims that the GRU took control of Crimea while the FSB coordinated operations in eastern Ukraine. It suggests that areas of cyberattack responsibility have been divided between GRU and FSB for more efficient resource allocation. Analyses of cyber forces indicate that in Crimea, like Georgia, Russia employed non-state actors; however, GRU played a more prominent role in this campaign, thus increasing Russia's cyber capacities.

Russian hybrid warfare methods in Ukraine showed similarities and improvements to the cyber operations employed in the Russo-Georgian war. In both cases, Russia used cyberattacks to gain information superiority and disrupt government operations before kinetic actions. Moreover, Russia utilised non-state cyber actors but included NATO allies in its targets list this time. However, The Crimea annexation operation showed that Russia employed more advanced cyber capabilities, with the GRU playing a larger role in offensive operations. It indicates Russia has become more adept at utilising cyber capabilities in its hybrid warfare campaigns.

Ukraine 2022

The Russian invasion of Ukraine differs from the conflicts in Georgia (2008) and Ukraine (2014). In February 2022, Russia sent 150,000 soldiers to invade a nation with 44 million population and one of the biggest regions in Europe (Bateman, 2022), making it the largest military conflict in the cyber-era (Wilde, 2022). Accordingly, cyberattacks were a component of this invasion, although experts claim that, like kinetic actions, cyberattacks did not achieve their primary objectives (Bateman, 2022). It prompted debates among scholars concerning cyberattacks' role in contemporary warfare and whether Russian cyber efforts fail to achieve their goals (Bateman, 2022). Analysis of Russian cyberattacks objectives and operational factors might provide some answers to these questions.

Russian cyberattack objectives against Ukraine share certain similarities, but also significant distinctions, with the Georgian War and the annexation of Crimea. Microsoft

(2022) reported that Russian cyberattacks in Ukraine targeted government and military functions, public trust and citizens' access to vital services. Thus, the primary targets of the cyberattacks were political leadership, military structures, and society. By strategically impacting society and undermining public trust in governmental leadership, Russia sought to diminish Ukraine's will to fight. Additionally, Russia launched massive data deletion attacks before and during the initial invasion stages, further increasing chaos (Bateman, 2022). Differently from previous conflicts, Russia aimed at Ukraine's critical infrastructure. On 23-24 February 2022, Russian hackers targeted the Ukrainian power grid (Khmelova, 2023). Thus, cyberattacks were deployed to destabilise Ukraine before and during conventional activities by achieving information superiority. Like previous conflicts, Russian cyberattacks aimed to weaken Ukraine's political leadership, military forces, and society. Yet, this time they additionally sought to damage its critical infrastructure.

Analysing the time operational factor, Russia began to shape the battlefield for kinetic operations earlier than in previous conflicts. Russian cyber-campaigns continued from 2014 until 2022, aiming to destabilise the Ukrainian government (Willett, 2022). Therefore, Russia had eight years to test and develop their cyber tools, while Ukraine also was learning, adapting and enhancing its cybersecurity. Furthermore, Microsoft (2022) reported that Russian threat actors began preparing for war in March 2021, targeting Ukraine-related organisations, acquiring first access to targets, and attempting to gain intelligence on Ukraine's military and international relations. Almost one year of preparation time is much longer than previous conflicts.

Apparently, Russia's cyber-planning time was extended due to large-scale war preparations. Similarly to previous conflicts, Russia massively intensified cyberattacks in Ukraine during the initial attack phase. Figure 2 shows that Russia attacked 22 organisations with numerous cyberattacks during the first six weeks of the war. However, in later weeks the number of cyberattacks significantly decreased. According to NATO threat analyst Black (2023), the Russian cyber force struggled to maintain access to Ukrainian targets and develop new access to strategically important targets within short timeframes and a constantly changing operational environment. These facts indicate that maintaining access to targets during a large-scale war dynamic operational environment was a significant challenge for Russian cyber forces.

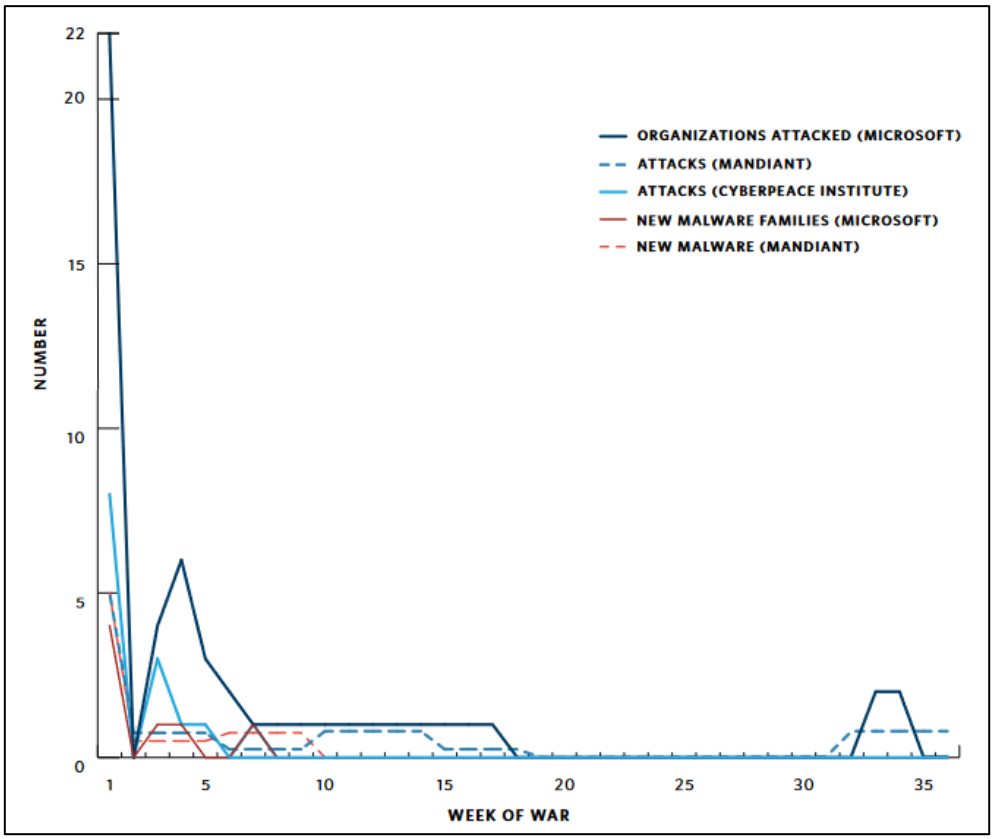


Figure 2. The Rise and Fall of Russian Destructive Cyberattacks in Ukraine. Source: (Bateman, 2022)

In the early stages of the war, Russian cyberattacks were synchronised in time and space with conventional operations. One hour before the invasion, the most damaging cyberattack was launched against Ukraine's Viasat satellite system (Strategic Survey, 2022). As previously, Russia began its offensive with communications disruption, but it employed more sophisticated tools this time. However, with international support, Ukraine could restore its communication channels. The US government and Space X swiftly provided numerous safe satellite communication Starlink connections (Strategic Survey, 2022). Furthermore, Microsoft provided valuable data on Russian cyberactivity and its coordination with conventional actions. Figures 3 and 4 illustrate how high kinetic and intensive cyber-actions supported the initial advance of Russia's offensive axes. Microsoft identified intensive cyberattacks in northern and eastern Ukraine and Kyiv, where Russian forces were advancing. Consequently, the failure of Russia's conventional operations at the war's beginning also diminished its cyber operations' efficacy. It highlights the interdependency of multidomain operations. To conclude, Russia used cyberattacks to disrupt communications and coordinated them with

conventional actions at the beginning of the war; nevertheless, Ukraine managed to withstand these attacks with enhanced cyber defence capabilities and international support.

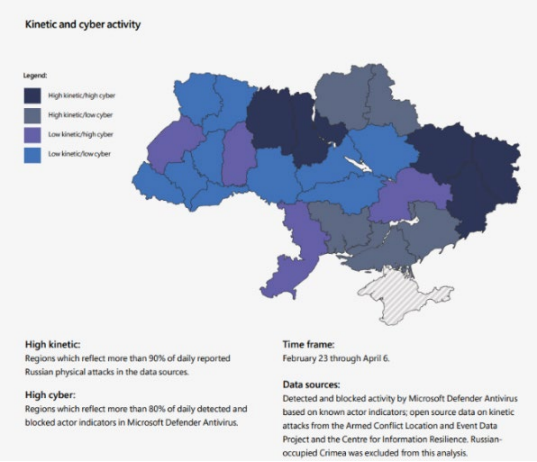


Figure 3. Kinetic and cyber activity. Source: (Microsoft, 2022)

Figure 4. Russian advancement as of 26 February 2022. Source: (Barney, 2022)

It is evident that Russia employed its cyber forces to support conventional operations. According to the Lithuania Regional Cyber Defence Centre (RCDC, 2022), at least eight Advanced Persistent Groups (APT) activities were identified and attributed to the GRU, FSB, SVR, and other Russian criminal organisations (Figure 5). GRU and criminals initiated the most critical attacks. Figure 5 shows that the APT28 – GRU unit and the Xaknet cybercriminal group conducted the most critical cyberattacks. In particular, the most damaging Viasat attack was attributed to GRU (Bateman, 2022). Hence, GRU was the primary cyber actor at the invasion's initial stage. Furthermore, Bateman (2022) noted that GRU focused on Ukraine, while FSB and SVR were active in international and domestic cyber-arenas, emphasising that Russian cyber forces were insufficient to impact a full-scale war significantly. Additionally, Russia's cyber capability limitation is seen from the decrease in cyberattacks after the first six weeks of the invasion (Figure 2). Consequently, large-scale and prolonged warfare requires far more resources than previous conflicts. These facts highlight Russia's comprehensive deployment of cyber forces to support this war yet suggest its limited resources and capabilities for sustaining a large-scale and protracted war.

Incident criticality level	Number of incidents	Tracked actors
Low	417	Armageddon, APT29
Medium	207	UAC-0051, UAX-0056
High	366	Sandworm, InvisiMole
Critical	316	APT28, XakNet

Figure 5. Russian APT actors mapped with incident number and criticality levels. Source: (RCDC, 2022)

Overall, Russian cyberattacks seek to weaken Ukraine's will to fight, disorganise its government and military, and gain information superiority, which is similar to that employed in previous conflicts. However, this war differs from earlier conflicts in certain ways that significantly affected Russian cyberattacks' efficacy. Russia had eight years to prepare its cyber forces for a massive invasion, with one year of active cyber preparation preceding kinetic operations, while Ukraine was also enhancing its cybersecurity. Russia's long planning period and use of more sophisticated tools suggest improved preparation compared to previous efforts. Additionally, Russia synchronized cyberattacks with conventional actions at the beginning of the war. However, with international support, Ukraine's enhanced cybersecurity has enabled it to resist Russian cyber efforts. Furthermore, the GRU was tasked as the primary cyber

force employed by Russia in Ukraine. This war highlights the limitations of Russia's cyber resources and capabilities in the face of more advanced and cyber-ready opponents supported by the international community.

Conclusion

Russian military doctrine, strategists' publications, and recent conflicts in Georgia (2008), Ukraine (2014), and Ukraine (2022) illustrate that cyberattacks will continue to be useful tools for Russia in shaping the battlefield. Information warfare has always been important to Russia, and it will continue to employ cyberattacks as one of its components. Russia utilises cyberattacks to gain information superiority by disrupting government operations and influencing society's willingness to fight before kinetic actions. Additionally, cyberattacks are intensified at the beginning of a war to exploit the element of surprise and create an atmosphere of chaos. Recent conflicts have shown that Russia is becoming increasingly skilled in using cyber capabilities. It employs various cyber operations, from less sophisticated DDoS attacks to more sophisticated attacks tailored against election systems, satellites, and critical infrastructure. Nevertheless, targeted countries have managed to limit the effectiveness of these attacks through cyber-defence efforts and international support, highlighting the significance of international cooperation and assistance.

Russia has demonstrated both the advantages and limitations of cyberattack employment. Traditional state borders do not bind cyberattacks, so Russia utilises them before kinetic actions and to influence international arenas outside the battlefield. Moreover, time and force are essential elements for successfully implementing cyberattacks, as it is a time-consuming and skilful process that restricts its effectiveness when confronting dynamic conventional warfare. However, Russia has shown a systematic approach to cyber preparation for conflicts, allocating several months for small-scale conflicts and a year for full-scale war while intensifying cyberattacks during the early phase of conventional offense.

The recent war has highlighted the limitations of Russia when it comes to large-scale warfare. The lack of Cyber Command and post-Soviet culture among its intelligence agencies seems to reduce its combat potential and efficient allocation of resources. Furthermore, Russia lacks cyber forces to efficiently cover military theatres and international and domestic arenas. Consequently, cybercriminals and hacktivists will

continue playing a role in Russian cyber campaigns. Nevertheless, Russia will assess its lessons from recent conflicts and continue developing its cyber capacities.

Additionally, Russian cyberattacks employment in recent conflicts demonstrated valuable lessons for contemporary warfare. Although cyber capabilities are increasingly important in contemporary warfare, they are not a shortcut to war. Modern warfare will always include cyber tools, but they won't be decisive. The cyber domain supports other domains, such as land, air, and sea, and should be coordinated to create synergy. However, when an operation fails in one domain, it impacts other domains as well. This was seen in the failure of Russia's conventional offensive, which affected the scope and impact of their cyberattacks.

Finally, the international community should continue supporting countries at risk in response to the threat of cyberattacks from malicious state actors, such as Russia. Support should focus on providing technical expertise and recommendations alongside initiatives that promote the exchange of information and foster trust and cooperation among public and private sectors and states. The situation in Ukraine demonstrates that a collective effort is essential for creating robust and resilient cyber security systems in the face of conventional and cyber aggression.

Bibliography

BAGGE, Daniel P. 2019. *Unmasking maskirovka: Russia's cyber influence operations*. New York: Defense Press, 2019. ISBN 978-0-578-45142-8.

BARNEY, Timothy. 2022. Maps show - and hide - key information about Ukraine war. *The University of Richmond.* [Online]. 4 April 2022. [Cited: 21 January 2023]. https://urnow.richmond.edu/features/article/-/21193/maps-show---and-hide---key-information-about-ukraine-war.html?utm_source=news&utm_medium=referral&utm_campaign=features-story

BATEMAN, Jon. 2022. Russia's Wartime Cyber Operations in Ukraine: Military Impacts, Influences, and Implications. *Carnegie.* [Online]. 12 December 2022. [Cited: 20 December 2022]. https://carnegieendowment.org/files/Bateman_Cyber-FINAL21.pdf

BLACK, Dan. 2023. Russia's War in Ukraine: Examining the Success of Ukrainian Cyber Defences. *The International Institute for Strategic Studies.* [Online]. 28 March 2023. [Cited: 30 March 2023]. https://www.iiss.org/research-paper/2023/03/russias-war-in-ukraine-examining-the-success-of-ukrainian-cyber-defences/

CHERAVITCH, Joe and LILLY, Bilyana. 2020. Russia's Cyber Limitations in Personnel Recruitment and Innovation, Their Potential Impact on Future Operations and How NATO and Its Members Can Respond. *The NATO Cooperative Cyber Defence Centre of Excellence.* [Online]. December 2020. [Cited: 17 December 2022]. https://ccdcoe.org/uploads/2020/12/2-Russias-Cyber-Limitations-in-Personnel-Recruitment-and-Innovation_ebook.pdf

CONNELL, Michael and VOGLER, Sarah. 2016. Russia's Approach to Cyber Warfare. *Defence Technical Information Center.* [Online]. 2016. [Cited: 15 September 2022]. https://apps.dtic.mil/sti/citations/AD1019062

DARCZEWSKA, Jolanta. 2016. Rosyjskie siły zbrojne na froncie walki informacyjnej: dokumenty strategiczne = Russia's armed forces on the information war front: strategic documents. *Centre for Eastern studies.* [Online]. 27 June 2016. [Cited: 14 Nowember 2022]. https://www.osw.waw.pl/en/publikacje/osw-studies/2016-06-27/russias-armed-forces-information-war-front-strategic-documents

EVEN, Shmuel and SIMAN-TOV, David. 2012. Cyberspace Attacks and Restraints. *Journal Storage.* [Online]. 2012. [Cited: 22 August 2022]. https://www.jstor.org/stable/resrep08940.5

GALEOTTI, Mark. 2014. The 'Gerasimov Doctrine' and Russian Non-Linear War. *In Moscow's Shadows.* [Online]. 6 July 2014. [Cited: 26 November 2022]. https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/

GILES, Keir. 2012. Russia's public stance on cyberspace issues. *The NATO Cooperative Cyber Defence Centre of Excellence.* [Online]. 2015. [Cited: 19 November 2022]. https://ccdcoe.org/uploads/2015/04/CyCon_2012_book_web_sisu.indd_.pdf

GOLDMAN, Emily and ARQUILLA, John. 2014. Cyber Analogies. *Naval postgraduate school.* [Online]. 2014. [Cited: 24 October 2022]. https://core.ac.uk/download/pdf/36732393.pdf

GOV.UK. 2022. Russia's FSB malign activity: factsheet. *United Kingdom government.* [Online]. 5 April 2022. [Cited: 21 January 2023]. https://www.gov.uk/government/publications/russias-fsb-malign-cyber-activity-factsheet/russias-fsb-malign-activity-factsheet

GREENBERG, Andy. 2019. *Sandworm: a new era of cyberwar and the hunt for the Kremlin's most dangerous hackers*. First edition. New York: Doubleday, 2019. ISBN 978-0-385-54441-2. HV6773.R8

HAKALA, Janne and MELNYCHUK, Jazlyn. 2021. Russia's strategy in cyberspace. *NATO strategic communications centre of excellence.* [Online]. 2021. [Cited: 24 September 2022]. https://stratcomcoe.org/publications/russias-strategy-in-cyberspace/210

HALL, Charles H. 2011. Operational Art in the Fifth Domain. *Naval war college.* [Online]. 3 May 2011. [Cited: 21 September 2022]. https://www.researchgate.net/publication/235087931_Operational_Art_in_the_Fifth_Domain

JASPER, Scott. 2020. *Russian cyber operations: coding the boundaries of conflict*. Washington, DC: Georgetown University Press, 2020. ISBN 978-1-62616-799-5. U167.5.C92

KHMELOVA, Ilona. 2023. Cyber, artillery, propaganda. General overview of the dimensions of Russian aggression. *State Service of Special Communication and Information Protection of Ukraine.* [Online]. 17 January 2023. [Cited: 17 February 2023]. https://cip.gov.ua/ua/news/kiberataki-artileriya-propaganda-zagalnii-oglyad-vimiriv-rosiiskoyi-agresiyi

KOFMAN, Michael, FINK, Anya, GORENBURG, Dmitry, CHESNUT, Mary, EDMONDS, Jeffrey and WALLER, Julian. 2021. Russian Military Strategy: Core Tenets and Operational Concepts. *The Center for Naval Analyses.* [Online]. 2021. [Cited: 10 October 2022]. https://www.cna.org/archive/CNA_Files/pdf/russian-military-strategy-core-tenets-and-operational-concepts.pdf

KOSTYUK, Nadiya and ZHUKOV, Yuri M. 2019. Invisible Digital Front: Can Cyber Attacks Shape Battlefield Events? Journal of Conflict Resolution. *Scholars at Harward.* February 2019. Vol. 63, no. 2, pp. 317–347. DOI 10.1177/0022002717737138. [Online]. 2019. [Cited: 18 November 2022] https://scholar.harvard.edu/zhukov/publications/invisible-digital-front-can-cyber-attacks-shape-battlefield-events

KOZLOWSKI, Andrzej. 2014. Comparative analysis of cyberattacks on Estonia, Georgia and Kyrgyzstan. *European Scientific Journal.* [Online]. November 2020. [Cited: 10 October 2022]. https://www.researchgate.net/publication/345883552_Comparative_analysis_of_cyberattacks_on_Estonia_Georgia_and_Kyrgyzstan

LAMBETH, Benjamin S. 1992. Desert Storm and its meaning: the view from Moscow. *RAND*. [Online]. Santa Monica, CA: Rand. A Project Air Force report. ISBN 978-0-

8330-1258-6. [Cited: 11 November 2022]. https://www.rand.org/pubs/reports/R4164.html

LEVI, Ron. 2022. Malicious Life: The Russian Business Network. *Apple Podcasts.* [Online]. 2022. [Cited: 18 December 2022]. https://podcasts.apple.com/lt/podcast/the-russian-business-network/id1252417787?i=1000586124675

LILLY, Bilyana and CHERAVITCH, Joe. 2020. The Past, Present, and Future of Russia's Cyber Strategy and Forces. In: 2020 12th International Conference on Cyber Conflict (CyCon). *The NATO Cooperative Cyber Defence Centre of Excellence.* [Online]. May 2020. [Cited: 16 September 2022]. DOI 10.23919/CyCon49761.2020.9131723, https://ccdcoe.org/uploads/2020/05/CyCon_2020_8_Lilly_Cheravitch.pdf

LONG, Gordon. 2013. Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in the Information Space (official translation). *Academia.edu.* [Online]. 2013. [Cited: 19 November 2022]. https://www.academia.edu/28009148/Conceptual_Views_Regarding_the_Activities_of_the_Armed_Forces_of_the_Russian_Federation_in_the_Information_Space

MAZANEC, Brian M. 2015. *The evolution of cyber war: international norms for emerging-technology weapons*. Lincoln: Potomac Books, an imprint of the University of Nebraska Press, 2015. ISBN 978-1-61234-763-9. [Online]. 2015. [Cited: 19 September 2022]. https://www.jstor.org/stable/j.ctt1d989jrKZ6718M39 2015

MEDVEDEV, Sergei A. 2015. Offense-deffense theory analysis of Russian cyber capability. *Naval postgraduate school.* [Online]. 2015. [Cited: 18 November 2022]. https://apps.dtic.mil/sti/pdfs/ADA620663.pdf

MICROSOFT. 2022. An overview of Russia's cyberattack activity in Ukraine. *Microsoft special report: Ukraine.* [Online]. 27 April 2022. [Cited: 10 November 2022]. https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd

PALOALTO. 2022. How to Break the Cyber Attack Lifecycle. *Palo Alto Networks.* [Online]. [Cited: 7 December 2022]. https://www.paloaltonetworks.com/cyberpedia/how-to-break-the-cyber-attack-lifecycle

PINGIOS, Anastassios. 2021. xorl %eax, %eax. *Russia's Cyber Operations Groups.* [Online]. 16 April 2021. [Cited: 4 December 2022]. https://xorl.wordpress.com/2021/04/16/russias-cyber-operations-groups/

RCDC. 2022. Report on the Russian Use of Offensive Cyber Capabilities in the Course of the Military Aggression in Ukraine. *Regional Cyber Defence Center.* [Online]. 2022. [Cited: 10 November 2022].

https://www.nksc.lt/doc/rkgc/Report_Russian_Use_of_Offensive_Cyber_Capabilities_in_UA.pdf

RF. 2010. The Military Doctrine of the Russian Federation. *Carnegie*. [Online]. 2010. [Cited: 15 November 2022]. https://carnegieendowment.org/files/2010russia_military_doctrine.pdf

SHAKARIAN, Paulo. 2011. The 2008 Russian Cyber-Campaign Against Georgia. *Military Review.* [Online]. 2011. [Cited: 17 December 2022]. https://www.researchgate.net/publication/230898147_The_2008_Russian_Cyber-Campaign_Against_Georgia12/17/2022

SOLDATOV, Andrei and BOROGAN, Irina. 2021. Russian Cyberwarfare: Unpacking the Kremlin's Capabilities. *The Center for European Policy Analysis (CEPA).* [Online]. 2021. [Cited: 4 December 2022]. https://cepa.org/wp-content/uploads/2022/09/Unpacking-Russian-Cyber-Operations-9.2.22.pdf

STINISSEN, Jan. 2015. A Legal Framework for Cyber Operations in Ukraine. *The NATO Cooperative Cyber Defence Centre of Excellence.* [Online]. 2015. [Cited: 14 January 2023]. https://ccdcoe.org/uploads/2018/10/Ch14_CyberWarinPerspective_Stinissen.pdf

STRATEGIC SURVEY. 2022. Russia's War in Ukraine What are the emerging military lessons? *Strategic Survey*. 4 December 2022. Vol. 122, no. 1, pp. 31–74. DOI 10.1080/04597230.2022.2145088. [Online]. 2022. [Cited: 6 December 2022]. https://www.tandfonline.com/doi/full/10.1080/04597230.2022.2145088

THOMAS, Timothy. 2004. Russia's Reflexive Control Theory and the Military. *The Journal of Slavic Military Studies*. June 2004. Vol. 17, no. 2, pp. 237–256. DOI 10.1080/13518040490450529.

VEGO, Milan N. 2009. *Joint operational warfare: theory and practice*. Newport, RI: U.S. Naval War College, 2009. ISBN 978-1-884733-62-8.

WALKER, Natalie. 2015. International Journal of Cyber-Security and Digital Forensics (IJCSDF) Vol. 4, No. 4. *International Journal of Cyber-Security and Digital Forensics (IJCSDF)*. [Online]. 30 November 2015. Vol. 4. [Cited: 18 November 2022]. https://www.researchgate.net/publication/306263976_IJCSDF_Vol_4_No_4

WARD, Amanda M. 2014. The Okhrana and the Cheka: Continuity and Change. *The College of Arts and Sciences of Ohio University.* [Online]. 2014. [Cited: 12 November 2022]. https://etd.ohiolink.edu/apexprod/rws_etd/send_file/send?accession=ohiou1398772391

WEBSTER. 1998. Definition of distributed denial of service. *Merriam-Webster dictionary.* [Online]. 1998. [Cited: 13 January 2023]. https://www.merriam-webster.com/dictionary/distributed+denial+of+service

WILDE, Gavin. 2022. Cyber Operations in Ukraine: Russia's Unmet Expectations. *Carnegie.* [Online]. 2022. [Cited: 20 December 2022]. https://carnegieendowment.org/files/202212-Wilde_RussiaHypotheses-v2.pdf

WILLETT, Marcus. 2022. The Cyber Dimension of the Russia–Ukraine War. *Survival*. 3 September 2022. Vol. 64, no. 5, pp. 7–26. DOI 10.1080/00396338.2022.2126193.

MAJ Denys YURCHENKO. Are 'we' NATO, the US, the EU, and the West to blame for the war in Ukraine?

Introduction

Russia and some in the West blame NATO for the war in Ukraine. In this version of the origins of the war, the USA and the West provoked Russia to respond. In Ukraine, Russia is fighting for vital security interests. While it is not surprising that Russians and Chinese politicians claim these statements as their own, it is surprising that they are also coming from Western scholars and senior officials.

This essay will not discuss arguments and statements provided by Russia, China, and other autocratic regimes. For them, such claims are no more than propaganda for the domestic audience. Yet, these are also arguments of scholars who are influential among the Western policy elite and shape the understanding of the general public about the war. These arguments are publicised in influential publications such as Foreign Policy and The New Yorker *(Mearsheimer, 2014, Chotiner, 2022)*. It is thus crucial to pay attention to them and see how they could be debunked.

From a practical point of view, this research paper deals with a topic that is important for USA, European and Ukrainian audiences. Properly understanding this challenging issue can help the Western world lose its sense of guilt and devise rational ways of dealing with authoritarian countries. For example, if China tries to start a war against Taiwan.

Ukrainians should also realise who is the guilty party in the war. This is essential because misunderstanding always leaves space for future manipulations. Currently, 64% of Ukrainians expect their country to join NATO and the EU within the next ten years *(Younis, 2022)* and, by so doing, entrench the country's democratic liberal orientation. Unfortunately, this number can rapidly decrease if arguments of seemingly respectable scholars go unchallenged, and it appears that the West is to be blamed for its misfortunes.

This paper aims to answer the question of whether 'we' NATO, the US, the EU, and the West are to blame for the war in Ukraine, examining three most common reasons: the enlargement of NATO; the expansion of the EU; and the weakness of the West. First, Russia and those who support it claim that the continuous growth of NATO is one of the biggest threats to the Russian Federation. Realists believe Russia started a brutal war in 2022 because NATO promoted Ukraine to join. Hence, Russian borders with NATO would increase, and NATO forces would be just 500 kilometres from the Russian capital – Moscow *(Chotiner, 2022)*.

The expansion of the European Union and the establishment of strong democratic values in Ukraine are presented by the school of realism as another threat to the Russian regime. This is seen as an extension of NATO enlargement and thus is one of the core dangers for Russia. This argument is also prevalent among Russian policymakers.

The final argument on the weakness of democratic systems seems to be different but follows a similar trend. Over the last sixteen years, there have been continuous discussions of the decline of democracies. *(Repucci, Slipowitz, 2022).* Western institutions such as NATO and the EU were weak and struggled after the COVID-19 pandemic and departure from Afghanistan. The last thing the West world wanted was to provoke Russia to start an invasion of Ukraine. Most believed that providing military aid and adopting tough sanctions against Russia would only accelerate the possibility of war.

This work will argue that the enlargement of NATO and expansion of the EU were not the causes of the war in Ukraine. Or rather, they were indirect causes as the internal needs of the Putin regime were at the centre of thinking and planning for the invasion. The seemingly opposite argument of the fault of the West in its failure to deter Russia will also be addressed. These arguments will be assessed in more depth in the following chapters, and conclusions and recommendations will eventually be made.

NATO expansion and Russian security concerns

The war in Ukraine did not start on 24th February 2022. It began in 2014 when Russia seized Crimea and started using its proxies in Donetsk and Lugansk *oblast* against the

Ukrainian Armed Forces. However, in 2022 Putin began a full-scale invasion, the most significant European war since the end of WWII *(Rand Corporation, 2022).*

Two leading proponents of the realist school of international relations – Distinguished Service Professor John J. Mearsheimer and Professor Stephen M. Walt claim that NATO provoked Russia to act in such a brutal way. Predictable that Russia would use their idea to justify the commencement of war *(MFA Russia, 2022)*. American journalist Anne Applebaum from The Atlantic publicly blamed Professor Mearsheimer for providing a narrative for Russian propaganda *(Applebaum, 2022)*.

Mearsheimer and Walt frequently say that NATO is guilty. In their view, the expansion of NATO was wrong from the beginning. After the collapse of the Soviet Union and the Warsaw Pact, the new rulers of Moscow did not deny U.S. troops staying in Europe. However, they did not favour the further enlargement of NATO. When two big rounds of NATO enlargement were conducted in 1999 and 2004, Russia was weak and could not protest.

In 2007 at the Munich Conference on Security Policy, Putin attacked NATO expansion. He claimed that NATO did not ensure European security but represented severe provocations. Additionally, Putin appealed for assurances from NATO General Secretary Mr Wörner that the NATO army would not deploy outside German territory *(The Official Website of the President of Russia, 2007).*

In 2008, four months after NATO declared that Ukraine and Georgia would become new members, Russia launched a war against Georgia and continues to control two separatist regions, Abkhazia and South Ossetia. Moscow sent a strong signal that further NATO enlargement is unacceptable. Alliance did not give up after these declarations and marched forward with Albania and Croatia in 2009 *(Mearsheimer, 2014).*

Then Professor Mearsheimer continued that after the Revolution of Dignity and the escape of former Ukrainian President Yanukovych, Putin received the chance to act. He seized Crimea and then connected it to Russia. It was easy because sixty per cent of the population were ethnic Russians, and they wanted to be separated from Ukraine *(Mearsheimer, 2014)*.

Next, he pressured the new Ukrainian government to show that Russia would not allow Ukraine to be part of the Western world. Also, he encouraged separatists in Donetsk and Lugansk *oblast,* sending them advisers and weapons and providing diplomatic support. Additionally, he deployed a massive army near the Ukrainian border and raised the price of natural gas *(Mearsheimer, 2014)*.

After the brutal Russian invasion of Ukraine in 2022, professor Mearsheimer did not change his views and believed that the NATO Summit in Bucharest was the *Rubicon* when the West started to provoke Russia. NATO also enhanced cooperation with Ukraine since 2014 and continued to neglect Russia's concerns. NATO became a core aspect of the strategy of turning Ukraine into pro-American liberal democracy *(Chotiner, 2022).*

Professor Walt is another famous member of the realism school of international relations. He fully supports Mearsheimer's idea that expanding NATO threatened Russia. The 2008 NATO Bucharest summit declaration that Georgia and Ukraine would someday become NATO members was a redline to Russian leaders. They treat Ukraine and Georgia differently than other countries who joined Alliance. The issue was not what the West thought about NATO enlargement. It told Russians repeatedly that it was no threat. The problem was that Russia thought it was a threat to them. Most Russian people believed that Ukraine joining NATO was a threat to Russia *(Munk Debate: Russia-Ukraine War, 2022).*

For Russia, the war in Ukraine is now a question of respect. It is the defence of vital interests. When great powers feel a threat, they start doing brutal things, even if they are democratic countries. United Nations and other international organisations cannot prevent them from starting illegal wars. The USA invaded Iraq in 2003 without UN Resolution, Russia is doing the same in Ukraine now *(Walt, 2022).*

Professor Walt goes further and compares the USA with Russia in conducting wars. For him, the USA started the war in Vietnam because its national interests were threatened. Additionally, the USA created and supported the rebel army in Nicaragua in 1980 after the former dictator was overthrown by revolution like former president

Yanukovych in Ukraine. Russia did the same when it supported and provided weapons to separatists in Ukraine *(Munk Debate: Russia-Ukraine War, 2022).*

Realists believe that NATO threatens Russia because it continues to grow and tries to include Ukraine and Georgia. According to them, Russia is a great power, and Eastern Europe is its *backyard*. Moreover, in his 2021 essay, Putin describes the Ukrainian and Russian peoples as one nation. Russia sees former territories of the Russian Empire as its sphere of influence *(Putin, 2021).*

Another idea that Russia and USA with NATO should divide Europe was in the draft of two security treaties between NATO and the USA, published by the Russian Minister of Foreign Affairs in December 2021. Their main concepts were ensuring Russian security interests by ceasing future NATO enlargement and withdrawing Alliance's forces from new members since 1997 *(The Official Website of Ministry of Foreign Affairs of the Russian Federation, 2021)*.

These theses look entirely plausible, but there are significant issues with the realist theory. As Radoslaw Sikorski argued: 'It is not very realistic. It helps Russia to define what its security reasons are. The test of theory should be predictive power.' According to realist theory, Russia cannot stay with more NATO members on its border. Thanks to Putin's aggression, two new countries: Sweden and Finland, will join Alliance soon. According to the logic of realism, Russia should now see these countries as threats, but Russia protested only modestly *(Munk Debate: Russia-Ukraine War, 2022).*

Even Putin acknowledged at a conference in Turkmenistan in 2022, "We do not have such problems with Sweden and Finland, which, unfortunately, we have with Ukraine. We have no territorial issues… no disputes… we have nothing that could bother us from the point of view of Finland's or Sweden's membership in NATO" *(Teslova 2022).* However, when Finland joined NATO, the Russian border with Alliance increased by 1 340 km (830 miles).

The Russian border with Alliance had stayed the same since 2004 when Latvia, Lithuania and Estonia became new members. Putin believes the main issue is not NATO enlargement but Russian – Ukrainian territorial disputes. However, Russia reaffirmed its commitment to Ukraine to respect the independence and sovereignty

and the existing borders of Ukraine by signing a Memorandum on Security Assurances in connection with Ukraine's accession to the Treaty on the Non-Proliferation of Nuclear Weapon Ukraine *(The Official Website of Verkhovna Rada of Ukraine, 1994).* Another remark for challenging the statement that NATO did not acknowledge Russian security interests during enlargement is the Ukrainian progress in joining the Alliance. Despite the great desire of Ukrainians to join NATO, there has been no considerable progress since the Bucharest summit in 2008. Even in 2019, Ukrainian President Petro Poroshenko signed a constitutional amendment committing the country to become a member of NATO and the European Union *(RFE/RL, 2019).*

One of the most significant achievements was the Enhanced Opportunities Partner status granted by NATO to Ukraine in 2020. In 2021 in 69 para of the Brussels Summit Communique, NATO reaffirmed the 2008 decision for Ukraine to become a member through a membership action plan *(The Official Website of North Atlantic Treaty Organization, 2021).* However, the timeline was not mentioned. It is possible to say that NATO has frozen the joining of Ukraine despite its willingness.

In conclusion, Putin claimed he did not argue with Sweden and Finland becoming members of the Alliance. Even though the land border between NATO and Russia increased twice from 1 215 km to 2 555 km. This Putin's statement challenged Mearsheimer's central idea of NATO Enlargement being a threat to Russia. Also, fifteen years after Bucharest Summit, Ukraine and Georgia did not become members of the Alliance. Both countries have also not received member action plans. NATO was cautious with this issue and did not provoke Putin. Russia did not see any threat regarding NATO. For Russian leaders, it is only a problem when Ukraine becomes a member of NATO because it will mean the success of Ukraine. This seems to be the biggest threat. The next chapter will explore this argument.

The Expansion of the European Union and Establishment of Democratic Values in Ukraine.

Mr Mearsheimer, in his already classic article "Why the Ukraine Crisis Is the West's Fault", wrote that the West's three-prong strategy provoked Russians to attack in 2014. In 2022 he repeated the same idea that NATO enlargement, EU expansion, and turning Ukraine into a pro-American liberal democracy provoked Putin to start an invasion

(Mearsheimer, 2014). NATO enlargement as the core idea was discussed in the previous chapter. It is time to analyse EU expansion and Ukraine's desire to become a democratic country as another reason for blaming the West.

Professor Mearsheimer tries to connect EU expansion with NATO enlargement. He says that in 2008, the EU established the Eastern Partnership program to integrate six former Soviet Union republics into the EU economy. He continues that Russia condemned such an initiative. Russian policymakers blamed the EU for creating a sphere of influence near Russia. For them, EU policy was a 'stalking horse' for NATO expansion. *(Mearsheimer, 2014).*

Then he claimed that the West wanted to spread its values and establish democracy in Ukraine. For example, Mearsheimer mentioned that since 1991 the US government had spent more than five billion American dollars to help Ukraine become a democratic state. This money was used to fund at least sixty projects, which mainly aimed to promote civil society in Ukraine *(Mearsheimer, 2014)*.

In the following sections, the professor repeats the Russian narrative that the White House funded the Revolution of Dignity in 2013 – 2014 because Victoria Nuland and John McCain visited anti-government demonstrations. So, Russians believed that the West played a significant role in Yanukovych's ouster. No wonder Russian leaders would not accept installing a pro-Western government in Ukraine and allow USA and EU to conduct social engineering in Russia *(Mearsheimer, 2014).*

Finally, in 2022 during public debates and lectures, professor Mearsheimer repeated and emphasised that Russia could not allow Ukraine to become a pro-Western liberal democracy. However, Putin could allow Ukraine to become a neutral prosperous country with the same attitude as the Western countries and Russia. According to Mearsheimer, the biggest threat to Putin was democratic Ukraine with a pro-Western government and integrated into the EU sphere of influence. *(Mearsheimer, 2022 and Munk Debate: Russia-Ukraine War, 2022).*

Mearsheimer and other critics of the EU expansion illustrate it as preparation for NATO enlargement. Also, they explain that the EU is not like a trade union but as an aggressive international actor who threatens vital Russian interests. Simultaneously

Mearsheimer mentions that European and Russian leaders use different playbooks and believe in different values. For the West, EU expansion aimed to implement liberal ideas and create a vast zone of peace in Europe. For Russia, it was intervention in its *backyard* because Putin and his subordinates believed in realpolitik.

Mearsheimer is wrong when he says that the EU helps to establish pro-American democracy in Ukraine. Also, he is wrong in explaining membership in the EU as the first step to NATO. Only 21 members of NATO are EU Members, and in the EU, there are states who did not join NATO. Russian leaders can present to their domestic population that the EU and NATO are the same. However, they know about their differences as they have a vast experience in cooperation with both organisations. Russia saw the European Union as a significant trade partner before 2014 and after. Even if trade between them decreased, still some EU members promoted deeper cooperation with Russia *(Siddi, 2022).*

The official Eurostat website supports this idea. It shows that in 2013, the Russian export of goods to the EU was €199 billion; in 2015, after the Crimea annexation, it was only €130.3 billion. After that time, this number never reached its result in 2013. Before the full-scale invasion, Russia managed to sell Europe goods for €158 billion in 2021. Natural resources were the core element in Russian export to the EU during this period. For instance, in 2021, Russian revenue for energy was €106,3 billion *(The Official Website of European Union, 2022).*

Mearsheimer is primarily right with one statement – that Western democratic values threatened Russia. However, they were a threat to the Russian regime. The same idea had High Representative of the European Union for Foreign Affairs and Security Policy / Vice-President of the European Commission Josep Borrell after he paid a visit to Moscow one year before February 24. *(The Official Website of European Union External Action Service, 2021).*

Putin and his circle began invasions in 2014 and 2022 with one aim to defend their regime in Russia. Putin's major existential threat was and remains the EU democratic values. For him, EU enlargement is not an issue as such. The problem is that Ukraine will become a thriving democracy. If Ukraine succeeds, the Russians will want the same. Putin cannot allow that *(Munk Debate: Russia-Ukraine War, 2022).*

At the beginning of the twenty-first century, several “colour revolutions” broke out in countries of the Russian sphere of influence. The most significant was Orange Revolution in Ukraine in 2004. After that event in Ukraine, a new pro-Western government was established. Its main idea was to incorporate Ukraine into the Western world by joining NATO first and then the EU *(Person, McFaul, 2022).*

This protest was a significant threat to Putin’s regime. Firstly, it undermined the core idea of the Russian ideology of great power. Putin believed that only Russia had a right to influence and control post-Soviet republics. The desire of Ukrainians to join the Western world destroyed the attractiveness of the Russian world. Secondly, according to Putin – Ukrainians and Russians are one nation *(Person, McFaul, 2022).*

Hence, if the revolution was successful in Kyiv, it could appear in Moscow. Such protests indeed began in St. Petersburg and other cities in 2011 after parliamentary elections. They were the biggest protests in new Russian history. Moreover, it was the first time Russians showed a great desire and capability to overthrow Putin’s regime *(Person, McFaul, 2022).* Dictators like Putin could not just go and live an average life. For them to be in power is not only a question of prestige but the question of life. According to statistics, eighty per cent of autocrats, after losing power, finished in prison or exile or were killed *(Frye, 2021, 43).*

Putin had a horrible experience regarding national protests, which he got in Dresden. In 1989 the Berlin Wall fell, and the communist regime in East Germany was destroyed. 36-year-old Putin, the KGB officer, was left alone and could see the full spectrum of East Germans’ fury. He had to burn secret papers “night and day” and wait for help. This event caused mental trauma for him *(Glasser, 2019)*.

So, a prosperous, democratic Ukraine with a strong freedom-loving society was an annoying example for Putin of the weakness of autocrats. Also, it could be an excellent example for the Russian population how to overthrow their dictator – *Putin the Great*. For Putin to be overthrown means losing all money, property, and even life. As was discussed in this chapter, Putin was afraid of democracy in Ukraine but not the expansion of the European Union.

Part 3 Weak West

In previous chapters, the West was analysed as an aggressive geopolitics player, which provoked Russia to invade Ukraine in 2014 and 2022. Although, I have already mentioned that the Western Policy of enlargement was not a leading trigger of the war. In this section the another side of the coin will be analysed – the Western failure to deter Putin.

The Russian President was not afraid to act brutally as he firmly believed that the West would excuse him as it did before. In 2008 Russian troops invaded the small country of Georgia and destroyed Georgian troops during five days war. As a result, NATO foreign ministers claimed cooperation was suspended until Russia redeployed its forces from Georgia *(De Haas, 2009).*

Russia, from its side, speculated that cooperation with NATO would be stopped completely. However, Moscow only suspended all activities in the framework of NATO's Partnership for Peace programme. On the other hand, cooperation in Afghanistan was not disrupted *(De Haas, 2009)*. That signalled that Russia tried to play its own game with Alliance.

In September 2008, France and Germany insisted on returning to cooperation with Russia. During an informal meeting in September, the Alliance's defence ministers showed they desired to continue cooperation with Moscow in some critical spheres. In March 2009, NATO's foreign ministers decided to renew formal collaboration with Russia in the NATO-Russia Council (NRC) format. It was an example of NATO's weakness because Moscow did not withdraw forces from Georgia, even though this was a primary requirement in the armistice plan in 2008 *(De Haas, 2009)*.

Finally, in June 2009, the Russian foreign minister participated in the NRC session, where both parties decided to recommence dialogue. One year later, Russian president Medvedev said that Lisbon Summit 2010 was historic in terms of its spirit and atmosphere *(Atlantic Council, 2010).* Moreover, NATO and Russia agreed to resume Theatre Missile Defence Cooperation *(The Official Website of North Atlantic Treaty Organization, 2010).*

Thus, it took Russia only two years to return to the world geopolitics agenda and continue close cooperation with NATO. The West did not want to isolate Moscow despite its aggressive behaviour against neighbours. Moreover, the Alliance wanted to enhance cooperation with Russia in the essential sphere as missile defence cooperation.

In 2014 Russia illegally seized Crimea and occupied territories in the Eastern part of Ukraine. As a result, NATO foreign ministers decided to suspend cooperation with Russia in different spheres. Also, at Wales Summit in 2014, the Alliance's leaders claimed Russia should withdraw its forces from Ukraine *(Boaru, 2019).*

During this Summit, NATO tripled the size of its NATO Response Force to over. 40 000 service members. Additionally, the Alliances decided to increase the number of aircraft in the framework of the Baltic Air Policing from 4 to 16 jets. Despite these actions, former NATO Chairman Petr Pavel said Russia could occupy the Baltic States in two days *(Kuczyński, 2019).*

The cooperation in the framework of NRC has never been suspended. NATO and Russia have conducted ten meetings since April 2016. General Secretary continued to meet with the Russian Foreign Minister, as did the Chairman of the Military Committee with his counterpart Chief of the General Staff of the Russian Federation *(The Official Website of North Atlantic Treaty Organization, 2022).*

NATO tried to deter and cooperate with Russia simultaneously. However, Russians did not see such actions as a policy of isolation. The main reason for the failure is different foreign policy cultures. In the West, negotiations are part of its consensus culture, which is essential for diplomacy. However, Russia treats talks as a weakness. Russian leaders believe that if they have enough power, they do not need to talk but can act *(Minzarari, 2022).*

Hence, not only did NATO fail to deter Russia, but the European Union also made the same mistake. After 2014, the EU posed sanctions against Russia. As a result, the trade between them declined. Also, the EU abandoned selling military equipment to Russia. However, an investigation found that a third of the EU member states sold

lethal and nonlethal weapons to Russia for €346 million *(Brillaud, Curic, Maggiore, Miñano Schmidt, 2022).*

Unfortunately, the leading European exporters were France and Germany, €152 million and €122 million, respectively. For example, France sold military equipment belonging to the category "bombs, missiles…" and different types of systems which were put into Russian tanks and aircraft. Germany sold mostly icebreaker vessels but also rifles and "special protection" vehicles as well. All these deals used loopholes in the EU regulations *(Brillaud, Curic, Maggiore, Miñano Schmidt, 2022).*

At the same time, both these counties were the main ideologists of ending the war in Ukraine in the framework of the Minsk Agreements. They believed war could be completed only by diplomacy and refused to sell lethal weapons to Ukraine. Even when USA intelligence declared many times that Russia would invade, Germany's leaders announced that they could send only five thousand helmets to Ukraine. Putin believed the EU and the most influential European states would not disrupt him.

Regarding the diplomatic isolation of Russia, the situation mainly remained the same. In 2015, the EU claimed its relations with Russia severely deteriorated. However, member states hoped cooperation on shared interests would be helpful when possible. In 2016, the EU wrote in Global Strategy for the EU's Foreign and Security Policy that Russia should respect international law. On the other hand, the EU stated that it would be ready to cooperate with Russia if common interests overlap *(Meister, 2022)*.

Finally, the EU High Representative/Vice-President Josep Borrell emphasised that before he paid a visit to Moscow in 2021, nineteen official delegations at ministerial or higher levels from EU Member States visited Russia in the last two years *(The Official Website of European Union External Action Service, 2021).* It was a clear signal to Putin that he was not a pariah and that he could undermine the unity between member states.

So, the EU and NATO were not united in their ambitions to deter Russia before February 2022. For example, French President Macron denied the possibility of a Russian invasion and visited Putin just a week before the war. *(Picheta, 2022).*

Simultaneously, NATO claimed that "We have no plans to deploy NATO combat troops to Ukraine...we are focusing on providing support," Stoltenberg said during his interview on January 30. "There is a difference between being a NATO member and being a strong and highly valued partner as Ukraine." *(RFE/RL, 2022)*

U.S. President Joe Biden made a similar statement that the United States would not send U.S. troops to fight for Ukraine. The United States has also sent the opposite signal by withdrawing U.S. military personnel and relocating its diplomats. The USA did not want to fight a real war for Ukraine, despite Putin's desire to fight for Ukraine because he believed its vital for him *(Walt, 2022).*

Ukraine was left face-to-face with Russia. US, NATO, and EU members were ready to provide mostly training and consultations. Some started sending lethal weapons to Ukraine just a month before the war, but there was a clear decision not to fight for Ukraine. Despite military aid from allies, it was still not enough to deter Russia from the invasion of Ukraine.

Conclusions and Recommendations

This work analysed different explanations for the war in Ukraine and the role that the West could have played in its commencement. Firstly, it discussed realists' ideas that Russia is a great power and that the West had to pay attention to its vital interests. It was found that NATO enlargement cannot be treated as a trigger for war because the Alliance carefully included new members and paid attention to Russian concerns. Also, Ukraine's progress in joining NATO was frozen, and some members continued to say that Ukraine should wait. Finally, when Finland joined NATO, the length of Russia's borders with NATO doubled, but Putin claimed that it was not an issue.

Regarding EU expansion as a continuation of NATO enlargement, it was mentioned that the EU for Russia used to be a significant trade market. Russia did not propose to sign any security agreement with the EU as it did with USA and NATO. For Putin, the biggest threat from the EU was democratic values and Ukraine becoming a prosperous state. It is only a question of staying in power and not being killed by an angry crowd.

Finally, it is possible to argue that the West was weak and failed to deter Russia. This statement could be used in future for manipulation. However, the West did not have a

legal commitment to fight for Ukraine, it was not part of NATO and the EU. On the other hand, the desire of Western politicians to negotiate was treated by Putin's circle as a weakness only because they had two different approaches to diplomacy. Western leaders could not believe that Putin would invade Ukraine and start a confrontation with the Euro-Atlantic community because they thought they were clear about the harsh sanctions which would follow such a move.

West did make a mistake in considering Russia a trade partner as any other. Indeed, national security interests should be considered every time, but European leaders tried to build a massive bubble of democracy which would eventually include Russia. They were wrong when they believed showing power would escalate the possible war. In 1991, when the Soviet Union fell, fifteen new countries appeared on the world map. Russia was one of them, the biggest state in the world had two directions of future development. Russians could build a prosperous democracy based on the country's human and natural resources. However, they had another choice to make a version of the Russian 18th-century empire with solid power and a disenfranchised population (*Clinton, 2022)*.

Unfortunately, Putin and others chose the second option and did not use high incomes to build a democratic state but used this money to create strong armed forces. His main goal was to receive revenge and rebuild the Russian Empire with a new tsar. At the same time, the West was drawing down resources and forces and did not develop them *(Person, McFaul, 2022).*

Russian invasion in Ukraine shows that preventing an autocrat's regime from war is not possible only by soft power. Such regimes do not care about possible casualties and economic crises. For them, such wars are a chance to increase their ratings and explain why citizens suffer. It also explains why law enforcement and armed forces receive so many resources. So, it is possible to stop people like Putin only by power.
To conclude, the West is not to blame for the war in Ukraine. It followed its values of democratic development and cooperation, hoping that Russian leaders also understood these values and the benefits of adhering to them. Western countries could be blamed only for complacency and neglecting the development of hard power to support their soft power advantage.

Bibliography

Agreement on measures to ensure the security of The Russian Federation and member States of the North Atlantic Treaty Organization. 2021. *The Ministry of Foreign Affairs of the Russian Federation.* [Online] 17 December 2021. [Cited: 12 November 2022.] https://mid.ru/ru/foreign_policy/rso/nato/1790803/?lang=en.

Applebaum, Anne. 2022. And there it is. *Twitter*. [Online] 1 March 2022. [Cited: 12 November 2022.] https://twitter.com/anneapplebaum/status/1498615856779177984.

Atlantic Council. 2010. Medvedev calls NATO-Russia summit historic. *Atlantic Council*. [Online] 6 December 2010. [Cited: 4 December 2022.] https://www.atlanticcouncil.org/blogs/natosource/medvedev-calls-natorussia-summit-historic/.

Boaru, Gheorghe. 2019. NATO-Russia Relations: Evolutions and Controversie*. Annals: Series on Military Sciences.* [Online] 2019. [Cited: 5 December 2022.] https://www.aos.ro/wp-content/anale/MTVol11Nr1Art.3.pdf.

Borrell, Josep. 2021. My visit to Moscow and the future of EU-Russia relations. *European Union External Action Service.* [Online] 7 February 2021. [Cited: 23 November 2022.] https://www.eeas.europa.eu/eeas/my-visit-moscow-and-future-eu-russia-relations_en

Brillaud Laure, Curic Ana, Maggiore Maria, Miñano Leïla, Schmidt Nico. 2022. EU Member States Exported Weapons to Russia After the 2014 Embargo. *Investigate Europe*. [Online] 17 March 2022. [Cited: 6 December 2022.] https://www.investigate-europe.eu/en/2022/eu-states-exported-weapons-to-russia/.

Chotiner, Isaac. 2022. Why John Mearsheimer blames the U.S. for the Crisis in Ukraine. *The New Yorker*. [Online] 1 March 2022. [Cited: 10 September 2022.] https://www.newyorker.com/news/q-and-a/why-john-mearsheimer-blames-the-us-for-the-crisis-in-ukraine.

Clinton, Bill. 2022. I Tried to Put Russia on Another Path. *The Atlantic.* [Online] 7 April 2022. [Cited: 7 December 2022.] https://www.theatlantic.com/ideas/archive/2022/04/bill-clinton-nato-expansion-ukraine/629499/.

De Haas, Marcel. 2009. NATO-Russia Relations after the Georgian Conflict. *Clingendael Institute*. [Online] April 2009. [Cited: 3 December 2022.] https://www.clingendael.org/sites/default/files/pdfs/20090000_cscp_artikel_mhaas.pdf.

Eurostat. 2022. Energy represented 62% of EU imports from Russia. *The European Union.* [Online] 7 March 2022. [Cited: 24 November 2022.] https://ec.europa.eu/eurostat/web/products-eurostat-news/-/ddn-20220307-1.

EEAS. 2021. Russia: Speech by High Representative/Vice-President Josep Borrell at the EP debate on his visit to Moscow. *European Union External Action Service* [Online] 9 February 2021. [Cited: 23 November 2022.]

https://www.eeas.europa.eu/eeas/russia-speech-high-representativevice-president-josep-borrell-ep-debate-his-visit-moscow_en.

Frye, Timothy. 2021. *Weak strongman: the limits of power in Putin's Russia*. *Princeton: Princeton University Press.* p. 43. [Online] 6 April 2021 [Cited: 26 November 2022.] https://press.princeton.edu/books/hardcover/9780691212463/weak-strongman.

Glasser, Susan B. 2019. Putin the Great. *Foreign Affairs*. [Online] September/October 2019. [Cited: 26 November 2022.] https://www.foreignaffairs.com/articles/russian-federation/2019-08-12/putin-great.

Korab-Karpowicz, Julian. 2017. Political Realism in International Relations. *Stanford Encyclopedia of Philosophy Archive.* [Online] 24 May 2017. [Cited. 19 November 2022.] https://plato.stanford.edu/archives/sum2017/entries/realism-intl-relations/.

Kuczyński, Grzegorz. 2019. NATO-Russia Relations: The Return of the Enemy. *Warsaw Institute.* [Online] 4 April 2019. [Cited: 5 December 2022.] https://warsawinstitute.org/nato-russia-relations-return-enemy/.

Mearsheimer, John. 2014. Why the Ukraine Crisis Is the West's Fault. *Mearsheimer* [Online] September/October 2014. [Cited: 12 November 2022.] https://www.mearsheimer.com/wp-content/uploads/2019/06/Why-the-Ukraine-Crisis-Is.pdf.

Mearsheimer, John. 2022. The causes and consequences of the Ukraine war. A lecture by John J. Mearsheimer. *YouTube* [Online] 16 July 2022. [Cited. 19 November 2022.] https://www.youtube.com/watch?v=qciVozNtCDM.

Meister, Stefan. 2022. A Paradigm Shift: EU-Russia Relations After the War in Ukraine. *Carnegie Europe*. [Online] 29 November 2022. [Cited: 6 December 2022.] https://carnegieeurope.eu/2022/11/29/paradigm-shift-eu-russia-relations-after-war-in-ukraine-pub-88476.

MFA Russia. 2022. The US & Its European Allies Share Most of the Responsibility for the Crisis. The Taproot of the Trouble is NATO Enlargement. *Twitter*. [Online] 28 February 2022. [Cited: 9 November 2022.] https://twitter.com/mfa_russia/status/1498336076229976076.

Minzarari, Dumitru. 2022. Failing to Deter Russia's War Against Ukraine: the Role of Misperceptions. *German Institute for International and Security Affairs.* [Online] April 2022. [Cited: 3 December 2022.] https://www.swp-berlin.org/en/publication/failing-to-deter-russias-war-against-ukraine-the-role-of-misperceptions.

Munk Debate: Russia-Ukraine War | Stephen Walt, John Mearsheimer v Michael McFaul, Radosław Sikorski. 2022. *YouTube* [Online] 12 May 2022. [Cited: 12 November 2022.] https://www.youtube.com/watch?v=EhgWLmd7mCo.

National Memorial to the Heavenly Hundred Heroes and Revolution of Dignity Museum, 2022. Heavenly Hundred. *Maidan Museum.* [Online] 2022 [Cited: 26 November 2022.] https://www.maidanmuseum.org/en/node/348.

NATO. 2010. NATO-Russia set on path towards strategic partnership. *NATO*. [Online] 20 November 2010 [Cited: 4 December 2022.] http://www.nato.int/cps/en/natohq/news_68876.htm.

NATO. 2021. Brussels Summit Communiqué issued by NATO Heads of State and Government (2021). *NATO* [Online] 14 June 2021. [Cited: 12 November 2022.] https://www.nato.int/cps/en/natohq/news_185000.htm.

NATO. 2022. NATO-Russia Realtions. *NATO.* [Online] 2022. [Cited: 5 December 2022.] https://natolibguides.info/nato-russia

Person Robert, McFaul Michael. 2022. What Putin Fears Most. J*ournal of Democracy*. [Online] April 2022. [Cited: 19 November 2022.] https://www.journalofdemocracy.org/articles/what-putin-fears-most/.

Picheta, Rob. 2022. Boris Johnson Claims France Was 'in Denial' Before Russia's Invasion of Ukraine. *CNN*. [Online] 22 November 2022. [Cited: 7 December 2022.] https://www.cnn.com/2022/11/22/europe/boris-johnson-ukraine-invasion-europe-comments-intl/index.html.

Putin, Vladimir. 2021. On the Historical Unity of Russians and Ukrainians. *President of Russia*. [Online] 12 July 2021. [Cited: 12 November 2022.] http://en.kremlin.ru/events/president/news/66181.

Rand Corporation. 2022. Russia's War in Ukraine: Insights from RAND. *RAND Corporation.* [Online] 2022. [Cited: 9 November 2022.] https://www.rand.org/latest/russia-ukraine.html.

Rankin, Jennifer. 2021. Ex-NATO Head Says Putin wanted to Join Alliance Early on in His Rule. *The Guardian*. [Online] 4 November 2021. [Cited: 12 November 2022.] https://www.theguardian.com/world/2021/nov/04/ex-nato-head-says-putin-wanted-to-join-alliance-early-on-in-his-rule.

Repucci Sarah, Slipowitz Amy. 2022. The Global Expansion of Authoritarian Rule. *Freedom House*. [Online] 2022. [Cited: 9 November 2022.] https://freedomhouse.org/report/freedom-world/2022/global-expansion-authoritarian-rule.

RFE/RL. 2019. Ukraine President Signs Constitutional Amendment On NATO, EU Membership. *Radio Free Europe/Radio Liberty* [Online] 19 February 2019. [Cited: 12 November 2022.] https://www.rferl.org/a/ukraine-president-signs-constitutional-amendment-on-nato-eu-membership/29779430.html.

RFE/RL. 2022. NATO Says It Won't Send Troops to Ukraine If Russia Invades. *Radio Free Europe/Radio Liberty*. [Online] 30 January 2022. [Cited: 7 December 2022.] https://www.rferl.org/a/ukraine-nato-troops-russia-invasion/31678264.html.

Siddi, Marco. 2022. The partnership that failed: EU-Russia relations and the war in *Ukraine*. *Journal of European Integration*. [Online] 18 August 2022. [Cited. 23 November 2022.] https://www.tandfonline.com/doi/full/10.1080/07036337.2022.2109651.

Teslova, Elena. 2022. Putin explains how Finland, Sweden membership in NATO different from Ukraine's. *Anadolu Agency.* [Online] 30 June 2022. [Cited: 12 November 2022.] https://www.aa.com.tr/en/russia-ukraine-war/putin-explains-how-finland-sweden-membership-in-nato-different-from-ukraines/2627019.

The Official Website of the President of Russia. 2017. Speech and the Following Discussion at the Munich Conference on Security Policy. *President of Russia*. [Online] 10 February 2007. [Cited: 10 November 2022.] http://en.kremlin.ru/events/president/transcripts/24034.

Treaty between The United States of America and the Russian Federation on security guarantees. **2021.** *The Ministry of Foreign Affairs of the Russian Federation* [Online] 17 December 2021. [Cited: 12 November 2022.] https://mid.ru/ru/foreign_policy/rso/nato/1790818/?lang=en.

Verkhovna Rada of Ukraine. 1994. Memorandum on Security Assurances in Connection with Ukraine's Accession to the Treaty on the Non-Proliferation of Nuclear Weapon. *Verkhovna Rada of Ukraine.* [Online] 5 December 1994. [Cited: 12 November 2022.] https://zakon.rada.gov.ua/go/998_158.

Walt, Stephen M. 2022. The West Is Sleepwalking into War in Ukraine. *Foreign Policy*. [Online] 23 February 2022. [Cited: 7 December 2022.] https://foreignpolicy.com/2022/02/23/united-states-europe-war-russia-ukraine-sleepwalking/.

Walt, Stephen M. 2022. Liberal illusions and the Russian invasion of Ukraine. *YouTube* [Online] 10 March 2022 [Cited: 12 November 2022.] https://www.youtube.com/watch?v=Plmn68XX7Iw

Younis, Mohamed. 2022. Most Ukrainians Expect to Join NATO, EU in Next Decade. *Gallup* [Online] 21 October 2022. [Cited: 9 November 2022] https://news.gallup.com/poll/403655/ukrainians-expect-join-nato-next-decade.aspx.

BEST ESSAY OF THE HIGHER COMMAND STUDIES COURSE (HCSC)

LTC Rene INNOS. Does deterrence work in the cyber domain?

Introduction

With state-to-state conflict increasingly extending into cyberspace as well, the question arises, to what extent the conventional theories that have been created with conventional conflict environments in mind, still apply. Deterrence theory is specifically relevant as it is one of the most common theoretical approaches states have implemented in their defence strategies.

There is significant academic debate over the applicability of deterrence theory in cyberspace. Largely there is a divide between academics. Some have achieved consensus over deterrence being possible to achieve in cyber and have more discussion over solving individual areas of issue like the proportionality of response and the problem of attribution. Others however are of the belief that due to the vastly different environment cyberspace provides, deterrence theory is not sufficient to apply for problem-solving and needs to be replaced (Lan, et al., 2010 p. 1). There is also discussion over whether cyber deterrence and its success depend on the general size and power of the state as they may need to rely on other domains to successfully execute their chosen deterrence strategy (Burton, 2018 p. 8).

Derived from this academic debate, this paper will examine the viability of deterrence theory in cyberspace regarding its core elements and their execution in cyber. The research questions that guide this paper are as follows:

1. What are the differences between the cyber domain and other domains?
2. What are the principles and core elements of deterrence theory?
3. Are the core elements of deterrence theory applicable to the cyber domain?

This research claims that “Deterrence purely in the cyber domain is not viable in the near future and needs to be supported by other domains if the speed and precision of the attribution of cyber-attacks are not improved”. The paper will begin by discussing the key differences that come with the cyber domain, followed by a deeper look at deterrence theory and how its core elements are expressed in cyber. Main effort will be devoted on element of attribution, as the vital component of successful deterrence strategy.

Cyberspace as a domain of deterrence

Cyberspace being used as a domain of conflict has significantly increased over time and cyber-attacks are growing in frequency, sophistication and impact (Burton, 2018 pp. 2-3). This could be explained by the fact that cyber weapons come with relatively low entry costs and high chances of success in comparison to more traditional means (Taddeo, 2017 p. 339). They are increasingly being used as the choice of means for state and non-state actors and it raises the question of what can be done to deter them. Cyber threats come in a wide range including attacks, espionage and disruption. In international law, there is much more ambiguity when it comes to the legalities related to protection and retaliation against cyber-attacks and that leaves a much more difficult task for state officials to combat (Nye, 2017 p. 47).

Deterrence theory creates a framework for the prevention of conflicts and it has been applied to the cyber field as well but there are problems. Arguably deterrence theory, in its current state, is not fit for the highly diverse and complex environment of cyberspace and should be transformed to consider a more comprehensive spectrum of threats and actors (Burton, 2018 p. 4). There are several fundamental differences between the characteristics of traditional and cyber conflicts. If a traditional conflict occurs mainly in the physical world, then cyberspace contains physical, logical and personal layer (Brantly, 2018 p. 40). When a conventional conflict scenario requires a prevailing military situation, identification of involved parties' strategies by rational choice models, positive attribution, and singular retaliation, cyber conflicts are much wider in the variety of characteristics. They are far more ambiguous as they can be non-kinetic, involve different combinations of state and non-state actors, and happen in a constantly changing, man-made environment that is much easier to manipulate (Taddeo, 2017 p. 339). The man-made feature of cyber is specifically emphasized also by Martin Libicki, who is one of the lead thinkers in the field and has said “Everyone concedes that cyberspace is man-made. This is what makes it different from its predecessors” (Denning, 2015 p. 9). This environment also relies on different vulnerabilities from traditional conflicts, as cyber weapons are designed to target elements within cyberspace and they can manipulate the space itself (Brantly, 2018 p. 40).

There also needs to be an important differentiation made between cyber-attacks made towards private entities (e.g. individuals, and companies) and at the state level. There are different actors, motives and courses of action related to either attack. Attacks towards private entities are primarily motivated by receiving payment (e.g. ransom attacks) or stealing data and by most states are considered to be a criminal matter. They are mostly perpetrated by criminal organizations or lone attackers with no discernible ideology and handled by the police with no wider state-level or media attention directed towards them. Attacks on the state level however are usually motivated by the desire to show that the perpetrator is capable of penetrating the state system. The purpose is more to create chaos within the state and outwardly show their weaknesses while sending a message of strength or warning about themselves. The perpetrators of state-directed attacks most commonly also have another motive like political gain (Burton, 2018 pp. 12-15). Due to the wider variety of potential perpetrators behind cyber-attacks, those motivations may not conform to the original cost-benefit analysis. Other motivations like ideological considerations, a need to cater for a domestic audience or national honour and sovereignty might take precedents over the potential costs of the attack and therefore deem any deterrence strategies ineffective (Burton, 2018 p. 6).

Deterrence theory

Deterrence is defined as “a coercive strategy based on conditional threats with the goal of persuading the opponent to behave in a desirable way” (Taddeo, 2017 p. 341). The goal of deterrence is largely to persuade the opponent to abandon their plans of attack by either increasing the potential costs of the attack to an unfeasible level or decreasing the perceived feasibility of the attack itself. It is characterized by elements of power and control between the two conflicting parties and involves both political and military facets. Deterrence developed in the aftermath of World War II, with the transformation of military power from just being a means to defeat the adversary or increasing the opposition's cost of war, to being a significant piece of bargaining power in avoiding war by coercion and intimidation (Taddeo, 2017 p. 341). Deterrence rose to its greatest relevancy around the Cold War when it was actively used between the US and the Soviet Union in regard to nuclear threats (Freedman, 2021 p. 3).

Deterrence theory can be roughly divided into two strategies - deterrence by denial and deterrence by punishment. Deterrence by denial strategy aims to deter action by

making it seem infeasible or decreasing the aggressor's confidence in achieving its objectives and making their aims seem unlikely to succeed (Freedman, 2021 p. 15). In a classical sense, it represents a situation where the aggressor reconsiders due to perceiving the opposition as too powerful and thereby lacking conviction in their ability to successfully attack. The most obvious way deterrence by denial is done in practice includes the demonstration and deployment of force in contested territories prior to an offensive. However, deterrence by denial should not only be equated with military balance and could also be presented in other forms like in cyber, as will be discussed later on. Deterrence by denial diminished in usage, especially during the Cold War when the conflict between the US and the Soviet Union where due to the nuclear threat deterrence by punishment was heavily favoured (Nye, 2017 p. 45). Deterrence by punishment can be understood as reflecting a credible threat of punishment to the perpetrator in order to change their cost-benefit analysis and discourage them from attack (Nye, 2017 p. 54). Plainly put, if the perpetrators do decide to attack the retaliation will be much greater than the benefits from the original attack received. The punishment can come in the form of military or in an extreme case nuclear response, but may also include heavy sanctions, global isolation etc. It is generally considered that when deploying a strategy of denial or punishment, the latter is riskier as well as extreme considering that there is a high chance of the perpetrator not trusting that the punishment is actually carried out and it usually comes with greater globally reaching consequences (Freedman, 2021 p. 16).

Core elements of deterrence

There are four core elements that are associated with deterrence theory - attribution i.e. the identification of the opponent, defence and retaliation, which are considered as types of deterrence and signalling which means that the defender is capable of signalling credible threats (Taddeo, 2017 pp. 340-342).

Attribution

Attribution is the key primary element that needs to be present for deterrence to be successful. Identification of the opposing party is important for any retaliation to be accurate and defence to be effective. Additionally, in legal terms, attribution is necessary for any retaliative actions taken to be justified. With attribution also comes the biggest problem related to deterrence as it is often very difficult to exactly and

accurately identify the perpetrators (Taddeo, 2017 p. 343). According to Libicki uncertain attribution weakens the whole logic of deterrence, as it has an impact on the cost–benefit analysis, meaning that the costs of identifying the wrong perpetrator might outweigh the benefits of any attribution. Therefore, before there can be any steps taken towards strategies of deterrence, attribution is key (Libicki, 2009 p. 43).

While attribution is complicated even in the context of traditional conflict, in cyberspace the issues rise to a new level with the best-case scenario of attribution being problematic, if not entirely impossible. It is well emphasised by a quote from the former US Deputy Secretary of Defense William Lynn when he said “Whereas a missile comes with a return address, a computer virus generally does not” (Nye, 2017 p. 50). With nuclear conflict, there is at least prior knowledge of countries that are nuclear powers and it already aids any attribution, but with cyber conflict, the pre-requisites needed to plan and execute an attack are much smaller, broadening the potential suspect pool (Nye, 2017 p. 45). That also leaves the field of technical information, which the analyst works with, open to ambiguity. In the virtual context, it is much easier to muddle the digital footprint and hide the origin of the attack as well as the number of perpetrators or groups behind it. It is also very probable that high-profile targets are under several attacks at once and with all these complications it is very difficult to investigate and confidently execute attribution strategies (Kwiatkowski, et al., 2022).

Due to the complicated digital nature of cyber-attacks, it is important for the attribution process to be technically detailed and precise. Perpetrators can easily deny any involvement and it is vital for the attribution to be accurate before any deterrence strategy can be applied (Burton, 2018 pp. 6-7). Therefore, the process involves many complex steps and aims to combine the three types of attribution - technical, legal and political, into as credible a narrative as possible. Through technical investigation, there is an attempt to identify the attacker, whose actions are then assessed to determine if they have broken international laws and through political attribution, it is then decided how the outcomes of the investigation are announced and tied to a specific party (Kwiatkowski, et al., 2022). Tool-based attribution which is characterized by “grouping together attacks that leverage the same unique malware families”, is also commonly used and has increased in difficulty over the years. Firstly, because many attackers have created homemade backdoors in order to only rely on open-source software, which makes them publicly available to use by anyone and cannot identify a single

threat actor. Additionally, there have been observations of a tendency to share tools and procedures between closely related, yet different perpetrators like groups within the same region or being sponsored by the same actor but targeting different sectors (Kwiatkowski, et al., 2022).

Another important complication is that cyber attribution is incredibly time-consuming. Evidence gathering, analysis and dissemination are slow and can take months. With the start of the Russian offensive towards Ukraine on the 24th of February 2022, a cyber-attack towards the VIASAT satellite ground stations was conducted. The attack was not attributed publicly to Russian intelligence services until May 2022 (Vicens, 2022). This is because attackers use disguises at the level, where even if there was knowledge about the technology or the IP addresses responsible, this information was hardly reliable and needed additional technical or intelligence verification. Concealment of actions makes cyber attribution very difficult and costly, with even the extensive effort deployed not guaranteeing unequivocal proof (Banks, 2021 pp. 1046-1048). Cyberspace is also drastically different in terms of the frequency of attacks. For example, according to Estonian Information Systems Authority, which is responsible for overall cyber defence in Estonia, there were 2672 attacks in the year 2022 alone, with disruptive effects for the users (Estonin Information System Authority, 2023 p. 13). When the frequency and time aspects are combined, it is easy to see why cyber-attacks have such a low attribution rate - there is not enough time to even unequivocally attribute one attack to an actor before a new one comes up.

There are severe privacy issues also associated with public attribution. Much of the evidence which could be publicized in order to prove the identity of the attacker, would reveal classified methods and sources. Still, there are frequent calls for greater transparency needed in technical attribution. Parallel construction, a process of using covert means like signals intelligence, illegal wiretapping and plain hacking, is a valuable process that may allow for covert discovery of the perpetrator and further post-discovery reconstruction. However, parallel construction is not always possible and therefore it might seem more beneficial to ambiguously attribute the attack to one party, without the provided evidence it only weakens the public view on attribution, but as the alternative would be no attribution it is a difficult choice to make (Kwiatkowski, et al., 2022).

Beyond the technical complications mentioned above, there are also international barriers that limit successful attribution in cyber. There is little consensus outlined in international law as to what constitutes sufficient proof for cyberattack attribution. It is also not clear whether attribution needs to be public and what are the appropriate consequences that cyber-attacks should carry pending successful attribution. More specifically there needs to be greater clarification around what legal rules should be applied when cyber-attacks affect or target civilians and their infrastructure outside the use of force and armed conflict thresholds (Banks, 2021 pp. 1054-1055). There are also significant cross-border differences in legal and law-enforcement practices that are taken towards cyber operations. This combined with the added unwillingness to cooperate between organizations, cyber attackers are acting with increased impunity, further lowering the credibility of deterrence (Bendiek, et al., 2015 p. 557).

Despite all the weaknesses, gradually there have been some efforts made in public attribution. The United States has periodically made efforts like in 2014 five people from the People's Liberation Army of China were indicted on economic espionage charges but were not able to be brought to trial and as the attribution was not backed up with sufficient evidence, the cyberattacks continued regardless of threats of prosecution even in 2017 and 2018. Beyond the US in 2017 there were some efforts made towards public attribution following the global WannaCry ransomware attack. Malware was spread to around 230,000 computers in more than 150 countries, which specifically affected the healthcare system of the UK, where hospitals had to cancel thousands of appointments and emergency departments were rendered unable to treat patients, leading to massive diversions of ambulances and patients (Banks, 2021 p. 1043).

Ultimately cyber attribution should be considered a complicated process that cannot be taken on a binary scale and needs to be assessed based on the quality with the acceptance that it is impossible to receive absolute certainty. The process is complicated by the consequences of publication combined with potential state or non-state attackers and a lack of clear legal frameworks on the international level that would support the response to a cyberattack (Assumpção, 2020). Finally, it is important to note that without effective attribution, there is no deterrence. Cyber attribution is a vital step for executing deterrence as it serves as a basis for any further response, especially in terms of what type of strategy is chosen and how to maintain a response

that stays within legal parameters. Without successful attribution, retaliatory action can only be taken on the basis of assumption and would most likely include other domains than cyber and actions of indirect retribution.

Defence and Retaliation

As previously mentioned, deterrence comes in the form of denial or punishment. Derived from it, there are two strategies that a state can take in the form of deterrence - either defence or retaliation. Defence is a strategy related to deterrence by denial and is essentially focused on “controlling the impact of an attack by preventing it or by rendering it ineffective” (Taddeo, 2017 p. 346). Nowadays, the strengthening of cyber security capabilities has been the preferred strategy for protecting states from cyber-attacks. There are official policies established and specialized organizations created, that are devoted to a better organization of the defence of states' own cyberspace. At the same time, cyber has been in constant growth and societies are increasingly getting dependent on information technologies. It creates increasing complications to successful defence as the area that should be protected is expanding rapidly. According to the International Telecommunication Union (ITU) statistics for the year 2022, there are 5.3 billion internet users in the world, which is 66% of the world's population. The growth compared to the year 2021 has been 6.1 per cent (International Telecommunication Union, 2022). Simultaneously, there has been a constant growth of cyber-criminal activities. Only in the first half of the year 2022, there were 2.8 billion malware attacks conducted worldwide (Nivedita, 2023).

Another complication with a purely defensive approach to cyber is that the defenders will always stay one step behind the adversaries (Grealish, 2023). The attacker has an inherent advantage as they can concentrate their effort on one attack vector or vulnerability, while the defenders must be able to protect against all known vectors simultaneously and at the same level, making it very resource demanding. Derived from this burden, in recent years, states have started to increasingly focus on widening the responsibility for cybersecurity to all of society and especially to the private sector. The role of the private sector in defence is growing as the services provided by them get more digitalized. The banking sector serves as a good example here. Additionally, the private sector is the main provider of basic ICT networks and technology starting from cloud computing and ending with simple software. As states become more skilled in organizing their defences, adversaries have started to search for new attack

opportunities through the ICT service providers, known as supply chain attacks. This in turn positions states in a new situation, where good international cooperation among the states in order to quickly react to security incidents, will become vital. For example, in the case of Estonia, the majority of software in use is maintained by US IT companies, like Microsoft, CISCO and others. Beyond just defence, increasingly to discourage state-owned or sponsored attacks, governments have started to be more vocal about retaliation.

Deterrence by retaliation or punishment rests on the threat or actual use of force that would follow an attempt of an attack and motivate the offender to change their plan. In order to change the calculus of the attacker, the threat of a severe counterattack in cyberspace must, first of all, be credible, and that causes a series of problems for state actors. First, for retaliation through cyberspace to be effective and timely one has to have presence in adversary networks beforehand (Brantly, 2018 p. 35). Although states are currently using cyberspace heavily for intelligence gathering, it still rises issues, as maintaining a presence in several adversaries' networks, just for retaliation purposes is resources demanding. After all, potential adversaries like all others, also invest constantly in cyber defence to keep their networks secured (Brantly, 2018 p. 45).

The proportionality question also comes to play here. On one hand, there is a big risk that a retaliatory attack can lead to unnecessary escalation by having an effect not only on the adversary systems but damaging friendly or outsider systems as well (Taddeo, 2017 p. 346). This has been previously observed, for example, in the aforementioned attack against satellite service provider Viasat at the beginning of the Ukrainian war. The attack did not only interrupt services in Ukraine but affected seriously the work of the electricity wind turbines in Germany. Additionally, a retaliatory attack could have unintentionally so severe consequences, that the adversary can interpret it as an armed attack which according to the UN Charter, grants them the right to respond directly in a conventional military sense, leading to further escalation. There have been attempts in the UN to agree on a threshold from where a cyber-attack towards a state will be recognized as an armed attack, but as of now, an agreement has not been reached. Therefore, even states with nuclear deterrence options, like for example the US and France, have stated in their cyber defence policies that attacks can receive a response not only through cyberspace but retaliation can be done by diplomatic,

economic or military means as well (Chen, et al., 2023 p. 69). This is a clear sign that especially regarding, any retaliation or defence actions, states are quick to include other domains in their strategy of responding to attacks, making originally set hypothesis more and more credible.

Signalling

The last core element of deterrence is effective signalling. Signalling is key in deterrence as the defender relies on it to alert prospective attackers of their knowledge about the impending attack and covey their response and strategy should it come to fruition. Signalling can come in two forms - general or tailored. General signalling refers to the country's wider spreading of its overall deterrence strategy through open statements, commitment and capabilities, while tailored signalling is directed at the perpetrator and is more purposive in its indication of possible targets of retaliation (Taddeo, 2017 p. 352).

Signalling, like within the context of traditional conflict, is also important in cyberspace. In any situation, deterrence activities have effect just if the adversary knows about them. Usually, it can be done as simply as communicating to the adversary the behaviour they deem undesirable, either in public or privately, and persuading them to stop (Meer, 2017 pp. 88-89). Especially if it is being done in public the goal of signalling is to name and shame the opposition and cause negative consequences to their reputation and repercussions in domains beyond cyber. Largely signalling has the ability to change the original cost-benefit calculus that makes cyber weapons and the domain as a whole so appealing. As attribution is considered difficult and weapons almost cost-free, the aggressors are used to a high degree of anonymity, but through signalling, this can change. This gives policymakers the ability to add an extra level of escalation before real retaliatory action is taken (Meer, 2017 pp. 88-89). One recent example of public signalling comes from US President Joe Biden, when during a 2021 summit in Geneva, he warned the Russian President Vladimir Putin by handing him a list of 'off-limits' sectors to digital assaults, that in case breached, would be met with a response from their significant cyber capabilities (Matishak, 2021). This type of public signalling can be very effective but only extends to state-to-state conflicts. As cyber is a domain featuring a variety of actors, including private groupings and individuals, signalling one's intentions to them can be more complicated (Smeets, et al., 2020). Additionally, not all states are too keen to reveal their intentions to defend and how, as

can be seen by the example of Germany and France. Both states have revealed that they have offensive capabilities but have left it unknown when and how these cyberweapons would be used and neither has also threatened their adversaries with them as a response to an attack (Smeets, et al., 2020).

Effective signalling is especially vital for clear communication from the defender to the perpetrator, to outlining the resolve to defend or retaliate and what concrete action will be taken (Fischerkeller, et al., 2017 p. 387). This response that is indicated must be credible. If the communication is not clear or is perceived as illegitimate, the opponent will not take it into account and cause the deterrence strategy to fail (Meer, 2017 pp. 88-89). Signalling in cyber is especially problematic, due to the secretive nature of cyber operations, and rational behaviour not being the default with the variety of actors (Smeets, et al., 2020). When the defender spells out concrete ‘red lines’ that should not be crossed by the perpetrator, in the case of an irrational opponent, they may be seen as deliberate goals. If the goal of the attack is to cause damage and mayhem with little regard to the cost it will bring, the defender spelling out areas that would lead to escalation would only further motivate them (Meer, 2017 pp. 88-89).

One of the issues with signalling in cyberspace is the “one use only” component. The first step in executing effective signalling would be issuing a threat to respond, which however gives the adversary a significant incentive to proactively reduce the promised costs of the threat and thereby mute the potential effect of the entire response (Meer, 2017 pp. 88-89). It means that it is impossible to effectively communicate a threat to a perpetrator without revealing significant information or knowledge about their weaknesses (Smeets, et al., 2020). This, however, can affect the retaliation efforts as it allows the perpetrator to remedy the issues and lead to the useful vulnerabilities now being closed. In short with signalling comes the consequence that any weakness found can only be exploited once (Fischerkeller, et al., 2017 p. 387). Overall, executing effective signalling to cyber attackers comes with the loss of valuable knowledge and leverage about the opposition and needs to be credibly backed up with capabilities and actions to be taken seriously.

Conclusion

Cyberspace proves to be challenging environment from deterrence point of view. On one hand cyberspace is globally in constant growth, on the other hand dependency of

societies from IT technology is on increase. At the same time cyberweapons with considerable power are in easy reach and anonymity of attackers is simply achievable. All this stretches cyber defenses. Still, it does not mean that states should give up in defense of cyberspace, as it is the bases from where proper deterrence strategy will be developed.

Attribution of the cyber-attacks, definitely at technical and preferably at political level, is the key to cyber deterrence. In order to have a proper response one needs to know from where and whom the attack comes from. Unfortunately, the ability to quickly and precisely point to an attacker is the biggest deficiency states have as of now. This in turn leaves attackers with a sense of impunity as retaliation if any will come with delay. In order to change the situation, states and the private sector in overall have to invest more into technologies what contribute to a faster attribution. Secondly, more emphasis has to be put on improving information sharing among all concerned entities, to lessen the chance of known attackers slipping through the cracks.

Due to the high risk that retaliatory attack through the cyberspace can have uncontrolled and unwanted consequences leading to escalation it is not a far reach to assume that in the case of a cyber-attack against a state entity, deterrence beyond the cyber domain will be considered. For states' leadership, it is, therefore, necessary to focus on developing an all-encompassing cyber deterrence strategy where cyber is an defined mean for retaliation but not inclusive, with that leaving door open for retaliation through other domains, like diplomatic, economic or even conventional forces.

Additionally, it is prudent for states to work on internationally developing more clear guidelines related to appropriate responses and attitudes states should have in regard to cyber-attacks. This development of internationally recognised norms will go a long way to support states' individual deterrence strategies in cyber and regulate appropriate action that can be taken outside of the cyber domain (Fischerkeller, et al., 2017 p. 393).

As a whole, more needs to be invested into the capabilities of deterrence through the cyberspace in order for it to work as required. Cyber defence should not be abandoned, but more effort needs to be invested to strengthen attribution and signalling techniques as well as further developing successful defence and retaliation strategies. Overall

deterrence still has a way to go in finding its role in comprehensive cyber strategy but has the potential to be a vital aspect of cyber defence if it can be well executed and backed up with credible support from other domains.

Bibliography

Assumpção, Clara. 2020. E- International Relations. *The Problem of Cyber Attribution Between States.* [Online] E-IR Publications Ltd, 6 May 2020. [Cited: 12 March 2023.] https://www.e-ir.info/2020/05/06/the-problem-of-cyber-attribution-between-states/.

Banks, William. 2021. Cyber Attribution and State Responsibility. *International Law Studies.* 2021, Vol. 97.

Bendiek, Annegret and Metzger, Tobias. 2015. Deterrence theory in the cyber-century. Bonn : Gesellschaft für Informatik, 2015.

Brantly, Aaron F. 2018. The Cyber Deterrence Problem. [ed.] R. Jakschis, L. Lindström T. Minárik. *2018 10th International Conference on Cyber Conflict CyCon X: Maximising Effects.* 2018.

Burton, Joe. 2018. Cyber Deterrence: A Comprehensive Approach? *ccdcoe.org.* [Online] April 2018. [Cited: 25 January 2023.] https://ccdcoe.org/uploads/2018/10/BURTON_Cyber_Deterrence_paper_April2018.pdf.

Chen, Sarah and Taw, Jennifer. 2023. Conventional Retaliation and Cyber Attacks. *The Cyber Defense Review.* 2023, Vol. 8, 1.

Denning, Dorothy E. 2015. Rethinking the Cyber domain and Deterrence. *Joint Force Quarterly.* 2015, Vol. 77, 2.

Estonin Information System Authority. 2023. Situation in cyberspace: A Year of Denial of-Service Attacks. *Cyber Security in Estonia 2023.* 2023.

Fischerkeller, Michael P. and Harknett, Richard J. 2017. Deterrence is not a credible strategy for Cyberspace. *Orbis.* 2017, Vol. 61, 3.

Freedman, Lawrence. 2021. Introduction—The Evolution of Deterrence Strategy and Research. [book auth.] NL ARMS. *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.

Grealish, Gerry. 2023. Securitymagazine.com. [Online] 1 February 2023. [Cited: 30 April 2023.] https://www.securitymagazine.com/articles/98844-defense-in-depth-protects-against-known-and-unknown-cyber-threats.

International Telecommunication Union. 2022. https://www.itu.int/en/about/Pages/default.aspx. *https://www.itu.int/hub/publication/d-ind-ict_mdd-2022/.* [Online] International Telecommunication Union, 2022. [Cited: 21 March 2023.] https://www.itu.int/hub/publication/d-ind-ict_mdd-2022/.

Kwiatkowski, Ivan, et al. 2022. kaspersky.com. *Securelist.com.* [Online] AO Kaspersky Lab, 22 June 2022. [Cited: 3 April 2023.] https://securelist.com/unpacking-technical-attribution/106791/.

Lan, Tang, et al. 2010. Global Cyber Deterrence: Views from China, the U.S., Russia, India, and Norway. New York : The EastWest Institute, 2010.

Libicki, Martin C. 2009. *Cyberdeterrence and Cyberwar.* Arlington : RAND Corporation, 2009.

Matishak, Martin. 2021. www.politico.com. *www.politico.com/news/.* [Online] Politico LLC, 16 June 2021. [Cited: 12 March 2023.] https://www.politico.com/news/2021/06/16/biden-cyber-russia-494957.

Meer, Sico van der. 2017. Deterrence of Cyber-Attacks in International Relations: denial, retaliation and signaling. *International Affairs Forum.* Spring, 2017.

Nivedita, James. 2023. *Security Audit.* [Online] 5 April 2023. [Cited: 9 April 2023.] https://www.getastra.com/blog/security-audit/cyber-security-statistics/.

Nye, Joseph S. 2017. Deterrence and Dissuasion in Cyberspace. *International Security.* 2017, Vol. 41, 3.

Smeets, Max and Soesanto, Stefan. 2020. Council on Foreign Relations. *cfr.org/blog.* [Online] Council on Foreign Relations, 18 2 2020. [Cited: 12 April 2023.] https://www.cfr.org/blog/cyber-deterrence-dead-long-live-cyber-deterrence.

Taddeo, Mariarosaria. 2017. The limits of deterrence theory in Cyberspace. *Philosophy &Technology.* 2017, Vol. 31, 3.

Vicens, AJ. 2022. *cyberscoop.* [Online] 10 May 2022. [Cited: 4 April 2023.] https://cyberscoop.com/viasat-hack-russia-uk-eu-us-ukraine/.

CAPT (N) Peeter IVASK. NATO Force Integration Units: Legacy and Adaption Challenges in the New European Security Situation after February 2022

Introduction

The Russian aggressive and destabilising actions against Georgia 2008 and Ukraine 2014 were demonstrating openly Kremlin imperialistic intentions. For the NATO eastern flank countries, it was strong signal of the military threat what Russia is presenting for the region. Moreover, it was also weakening for Alliance, which stated in Wales Summit 2014 that Russian actions have fundamentally challenged a vision of free and peaceful Europe. As response to the Russian actions Alliance leaders approved Readiness Action Plan (RAP), which included measures to the continuing need for assurance of Allies and adaptation of the NATOs military posture. (Wales Summit, 2014 p. 1; 6)

One of the measures in RAP included enhancement of the NATO Response Force (NRF) by introducing Very High Readiness Joint Task Force (VJTF) and creation of the NATO Force Integration Units (NFIU). NATOs response on continued Russian aggressive rhetoric did not satisfy Baltic states and Poland (Fryc, 2016). There were several reasons which created doubts in these countries on why NRF and consequently NFIUs were not providing expected assurance from Russian threat (Stoicescu, et al., 2016). In 2016, NATO introduced enhanced Forward Presence (eFP) and multinational battalion size battlegroups were stationed in Baltic states and Poland. What influence introduction of the eFP had for NFIUs will be described later in this article. The focus of the article will be on the NFIUs doctrinal mechanisms and therefore, it will not argue over effectiveness of deterrence.

On 24th of February 2022 Russian open and brutal attack against Ukraine has made significant changes in NATOs strategy. The aftermath of that has even shifted neutral Sweden and Finland to apply for NATO membership. On 4th of April 2022 Finland signed Washington Treaty and Sweden will very likely follow soon.

So, what is the adaptation challenge of NFIUs? While NFIUs have already been operating for several years there is barely any research or written articles evaluating the role and capabilities of the units. Introduction of the NATO New Force Model (NFM)

(Madrid Summit, 2022) and the concept for the Deterrence and Defence of the Euro-Atlantic Area (DDA) (Bauer, 2022) has led to the discussions over role and value of the NFIUs. Moreover, the NFM is meant to replace the current NRF in which NFIUs are conceptual part. Alliance plan to improve readiness and responsiveness of the organisation is stretching even further national resources and therefore the relevance of the NFIUs has been questioned. How that drastic change in European security and NATOs adaptation have influenced the NFIUs will be reviewed in the current article.

Limited understanding of the NFIUs roles and capabilities within NATO and hosting nations aggravating the fair assessment of the units' value. Recognising this gap in knowledge, the following article aims to answer the question 'What adaption challenges NFIUs have in the new European security situation after February 2022?'. The article is divided on two parts. In the first part it is reviewing the adaptation of the NATO and new conceptual initiatives based on approved Alliance strategies and decisions made during the Summits. It introduces the legacy of NFIUs based on RAP aims and concepts. The article is presenting the eFP as one of the initiatives to improve NATOs responsiveness in the worsening security situation. In the second part of the analysis article focuses on the research problem, evaluates the NFIUs current roles based on the empiric survey and on assessment of the strategic documentation for the NATO adaptation. Along with the summary the article provides suggestions for future decisions concerning the NFIUs adoptation.

Research Method

To assess the research problem, whether NFIUs need to adapt in the new strategic environment author analysed NATO strategic documents and doctrines from Wales Summit to the resent Summit in Madrid. To assess the role of NFIU in the concept of assurance and deterrence measures author reviewed different threat assessments and articles. Author also conducted an empiric survey with all currently active NFIU commanders and received answers from four NFIUs.

The first part of the questionnaire was focussing on the tasks NFIUs are executing currently and what could be roles of the NFIUs to meet NATO 2022 Strategic Concept core tasks in the future. Two main questions as 'What are the tasks that your respective NFIU is executing throughout a year?' and 'What could be roles of the NFIUs to meet NATO 2022 Strategic Concept core tasks in support of the DDA concept and the

NFM?' were used for comparison analysis. The questions had nine pre-defined answer options and possibility to add any other tasks what respective NFIU is performing. All options of answers were based on the main mission and tasks of the NFIUs described in article. The survey question five focuses on the shortfalls of the NFIUs and provides basis for further analysis for necessary improvement. The stated question 'What should be improved/changed to adopt NFIUs for the future roles?' had eight answer options on which NFIU commanders had to choose five most relevant based on their experience.

The question six of the survey was looking specifically at the command-and-control relationship with the purpose to assess the subordination level of the units from practitioners' perspective. In the possible answer options, all levels of operations were presented. Joint Support and Enabling Command (JSEC) was placed specifically to represent strategic level of operations as Standing Joint Logistic and Support Group HQ (SJLSG), which by doctrine is the Logistics Theatre Component Headquarters (NATO AJP-01, 2023 p. 117), has been linked with it (NATO Fact Sheet JSEC, 2021). Two answer options, which represented operational level were Joint Force Commands (JFC) and Joint Logistic and Support Group HQs in Brunssum, The Netherlands, or in Naples, Italy which were established by JFCs following the NATO Defence Ministers decision in February 2018 (Joint Force Command Brunnsum, 2020). Option of answer for tactical level presented Multinational Corps or Division.

The NATO adaptation and NATO Force Integration Units legacy

To understand the NFIUs role this chapter will describe NRF concept, NFIUs basic organisation, and capabilities. The RAP provided coherent and comprehensive package of necessary measures to the challenges posed by Russia while responding to the risks emanating from the Middle East and North Africa. The assurance measures are flexible and scalable military presence on rotational basis. The adaptation measures included enhancement of the NRF by improving responsiveness of the forces. The new NRF included the VJTF and establishment of the NFIUs, as in-place enablers on the territories of the eastern NATO members. (Wales Summit, 2014 pp. 6 - 8) Those NFIUs have task to improve coordination between NATO and national forces, support exercises and any Alliance deployments needed (NATO Readiness Action Plan, 2016). Planned reconstruction of the NRF concept introduced VJTF as a

‘spearhead force’. This adopted approach has a brigade-sized unit in high readiness to move at five to seven days of notice. One of the battalions of VJTF must be ready to deploy within two to three days (Fryc, 2016 p. 49). To achieve such a short response time not only forces must be in higher readiness, but also preparation of deployment has to be planned and comprehensive exercise programme should be conducted. To accomplish requirements of rapid deployment NATO introduced NFIUs as in-place enablers to facilitate and support the movement of the VJTF. From the NATOs perspective creation of the NFIUs had dual purpose, first to facilitate deployment and secondly to provide non-escalatory persistent presence of NATO in the Alliance eastern flank. In 2015 NATO launched the JUMP-series exercises, which aim was to test VJTF and ensure that concepts and procedures will work in the event of a real crisis. That included also testing the concepts behind the NFIUs. (SHAPE Public Affairs Office, 2015) Therefore, establishment of the NFIUs was vital element of the RAP adaptation measures and for entire VJTF concept. Moreover, for every year VJTF has different leading nation which is switching in accordance with the rotation plan (Joint Force Command Brunssum, 2022). Consequently, it requires annual renewal of existing deployment plans and exercises for assigned units. To sustain that very short deployment time for VJTF extensive preparation, constant coordination, situational awareness, and planning of reception, staging and onward movement (RSOM) is paramount.

In 2015, six NFIUs were inaugurated in Bulgaria, Estonia, Latvia, Lithuania, Poland, Romania and two more were established 2016 in Hungary and Slovakia (NATO Fact Sheet NFIU, 2015).

NFIUs are small multinational units which have headquarters type organisation. The main mission for Units is to strengthen collaboration between national forces and the NATO high readiness forces by providing broad planning support to facilitate rapid deployment of Allied forces and together with host nations to identify logistical networks, transportation routes and supporting infrastructure (SHAPE Fact Sheet). NFIUs are manned with 40 military personnel on which half is provided from host nation and half by allied contributing nations. This construct of the organisation provides wide area of military expertise and experience for units (Botik, et al., 2022 p. 74). Although, ‘Joint by nature’ NFIUs are part of the NATO Force Structure and subordinated to the tactical level land element. Being part of the NATO Force Structure gives Units full

access to different NATO Communications and Information Systems (CIS) and functionalities. Majority of the NFIUs with exception of Poland and Hungary are co-located with host nation joint headquarters in the capital cities which is vital for liaising and coordination of activities. (Botik, et al., 2022 p. 73). It also provides unique opportunity to establish networks necessary for exchange of information and maintaining situational awareness. Understanding of the domestic affairs and maintaining situational awareness is crucial element of assisting and supporting planning of the exercises, operations, and deployments. Being 'Joint by nature' NFIUs have a unique position to cooperate with all actors in the country with direct access to all military command levels from strategic, to tactical level and associated civilian partners.

What has Enhanced Forward Presence Changed in 2016 - 2018?

Even though, the RAP made considerable changes in NATOs force posture and Alliance was moving away from reassurance to more responsive deterrence it did still not meet expectations of the Baltic states and Poland (Fryc, 2016 p. 46). Estonia had serious doubts over the actual employment of the VJTF. Even, if the spearhead battalion had 24-hour notice to move requirement the rest of the unit supposed to be ready in seven days. This timeframe was only the readiness for the deployment. The time which is needed for deployment as such must be added to that. As VJTF was not linked to the specific operational area there was no possibility for pre-positioning logistics materials or equipment and because of that movement of the unit from longer distances was even bigger challenge. In addition, the decision of the deployment was not automatically granted to SACEUR but required North Atlantic Council decision. (Stoicescu, et al., 2016 p. 9) Therefore, during the 2016 Warsaw Summit a renewed strategy of deterrence and defence was approved. Significant decision on establishment of the Enhanced Forward Presence (eFP) in Poland and three Baltic states and Tailored Forward Presence (tFP) in Romania, Bulgaria and Turkey was made. These forces make a first line of defence together with host nation forces to deter and defend from Russian aggression. (Mercier, 2018) The battalion size units were commonly characterized as 'a tripwire' in case of incursion to trigger Alliance collective response. While the new approach was attractive it has several practical constraints. The eFP is not a NATO mission, although enabled by NATO. During the 2016 Summit it was decided that individual eFP battalions will be integrated into their

respective host nation brigades and NATO has authority only over selected aspects on eFP forces. The framework nations are responsible for its own battlegroups and relationship with their host country, including the force generation and strategic planning. (Leuprecht, 2019) In reality battlegroup has three lines of command which are, NATO command line, national structures of command of the contributing nations, and the line of command in the host nation affiliated unit. That made the structure and command and control arrangements particularly complicated (Luik, et al., 2017). However, from the responsiveness perspective eFP battlegroup model provided highly respected forward presence and quick response to the emerging threats when NATO's collective defence mechanism may take time. It also provides framework nations opportunity for pre-emptive deployment of additional capabilities for assurance and deterrence. NATO's fastest response to reinforce nations and eFP battlegroups would be a deployment of the NRF 'spearhead' VJTF facilitated by respective NFIU (Leuprecht, 2019). Unfortunately, integration of the battlegroups with host nation brigades and establishing direct coordination with hosting country led framework nations to bypass the NATO chain of command. The NFIU's who were introduced to facilitate deployment of Allied forces are often not involved in rotations and troop movements of the eFP battlegroups. Awkwardly, one of the often-misinterpreted statements is that NFIUs being initiated by RAP are part of the eFP concept (Leuprecht, 2019 p. 6). NFIUs were not linked to approved eFP concept and remain with mission to facilitate deployment of NRF forces.

New Security Realm in Euro – Atlantic Area (2014 - 2023)

Although, Alliance has started adaptation and assurance of the member states already in 2014 Wales Summit the NATO's Strategic Concept was still from 2010. The assessment of the security environment in 2010 concept was stating that the Euro-Atlantic area is at peace and the threat of conventional attack against NATO territory is low. The focus of the threat perception was put on the terrorism, proliferation of weapons of mass destruction, resilience of the vital communication and transportation routes, technology related trends and cyber. (NATO Strategic Concept, 2010) At the same time Russian threat perception in the Baltic States remained still high. Based on the analysis and the Russian strategic exercise Zapad 2017 it was assessed that Russia continues using military pressure against Estonia, Latvia, and Lithuania (Estonian Foreign Intelligence Service, 2018 p. 18). In the annual report 2022 Estonian

Foreign Intelligence Service stated that military pressure and threats of war have become key foreign policy tools for Russia. The escalation on Ukraine's borders deteriorates the security of Europe as a whole and the level of military threat across Europe will rise. Therefore, Estonia must prepare for sustained military pressure from Russia (Estonian Foreign Intelligence Service, 2022 p. 9). It was obvious that the measures made by Alliance were not satisfying Baltic States and effectiveness of Alliance deterrence and assurance could be argued (Arnold, 2016).

On 24th of February 2022 Russia launch open military offensive against Ukraine and violated the norms and principles of European security order. As a response NATO approved new strategic concept in June 2022. The assessment of the strategic environment among other issues is stating clearly that the Russian Federation is the most significant and direct threat to Allies'. It seeks to establish spheres of influence and direct control trough coercion, subversion, aggression, and annexation. Russia has also proven willingness to use force to pursue its political goals and undermine the rules-based international order (NATO 2022 Strategic Concept, 2022).

NATO 2022 strategic concept defines three core tasks. Most relevant tasks for this article are under the Chapter of core task Deterrence and Defence. It defines that NATO will continue significantly enhance its deterrence and defence and ensure a substantial and persistent presence on land, at sea, and in the air. This includes also robust in-place combat-ready forces and enhanced command and control arrangements. Improvement of ability to reinforce any Ally and continue to enhance the collective readiness, responsiveness, deployability, integration and interoperability of NATO forces. Adaptation of the NATO command structure for the information age and enhance cyber defences, networks, and infrastructure. Within area of crisis prevention and management, NATO will ensure that necessary resources are available, and it continues contributing to stability. On cooperative security task NATO values practical cooperation with partners, will contribute to stability and enhance our security at home. (NATO 2022 Strategic Concept, 2022)

In parallel with Strategic Concept NATO has introduced several new concepts. Madrid Summit approved New Force Model (NFM) which will strengthen and modernise the NATO Force Structure. This NFM will be basis to resource new generation of military plans (Madrid Summit, 2022). On his interview for Reuters NATO Secretary General

Jens Stoltenberg said NATO in future would have ‘well over 300,000’ troops on high alert, compared to 40,000 troops that currently make up the alliance's existing quick reaction force, the NATO Response Force. The NFM is meant to replace the NRF and ‘provide a larger pool of high readiness forces across domains, land, sea, air and cyber, which will be pre-assigned to specific plans for the defence of allies.’ NATO combat units on the alliance's eastern flank nearest Russia, especially the Baltic states, are to be boosted to brigade level, with thousands of pre-assigned troops on standby in countries further west like Germany as rapid reinforcements. (Stoltenberg, 2022) NATO NFM has 3 tiers approach. Tier 1 which will be up to 10 days readiness will include over 100 000 soldiers. Tier 2 is planned to have 200 000 soldiers in 15 – 30 days readiness and Tier 3 will be at least 500 000 in 30 – 180 days readiness (NATO New Force Model, 2022).

NATO new Strategic Concept is followed by the concept for the Deterrence and Defence of the Euro-Atlantic Area (DDA), and the NATO Warfighting Capstone Concept (NWCC). The process of further developing and implementing the DDA ‘family of plans’ is in progress, and it has been already put successfully to the test. (Bauer, 2022)

By introducing the NFM Alliance has increased substantially the number of troops to be deployed. Especially, pre-assigned units on standby to reinforce countries nearest to Russia from the country’s further in west. Binding forces to specific plans improve the responsiveness of the Alliance and adjusting the shortfalls of the NRF concept. Nevertheless, the requirement to plan and support deployment of those forces remains and even increasing. As the NFM force package includes land, sea, and air capabilities the support of the deployment is definitely joint by nature and linked directly to the operational level.

Derived Conclusions from The Research

The following Chapter will provide analytical conclusions on the conducted research and provide outcome of the survey. The evolution of the NATO strategic documents and developed concepts showing constant improvement of NATOs deterrence posture and assurance measures. Russian growing aggressive behaviour and direct military intervention in neighbouring countries have triggered several responses from Alliance.

Improvement of the NRF and introduction new VJTF concept including NFIUs was one of many. Although, on strategic level the concept looked reasonable, while practical implementation was not fully exploited to achieve its expected outcomes. The practical difficulties and NATO cautiousness to escalate situation was creating doubts in Baltic states and Poland on the effectiveness of the entire VJTF concept. Therefore, the eFP as real presence of the NATO fighting units in land domain was welcomed in much higher enthusiasm in eastern flank countries. Beside the complicated C2 and being not a NATO mission, it was presenting the real commitment of the Alliance members to contribute deterrence and if needed to defend NATOs eastern border countries. Limited NATO authority over the eFP and C2 outside of the NATO Force Structure created parallel system for rotations and deployments of the units. That solution was compromising construct for framework, nations, host nations and NATO, but it left NFIUs out from common doctrine.

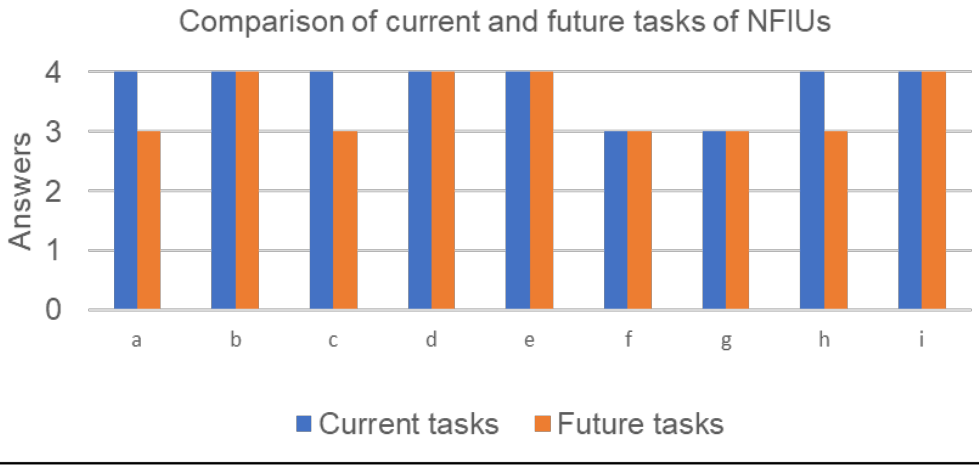
With the introduction of the NFM NATO is significantly increasing the number of troops to be deployed. Therefore, relevance of the support and facilitation of deployment is still accurate. NFM will be pre-assigned force tied to specific plans for the defence, and areas of responsibility which is different in principle from the NRF construct. With new approach, adaptation, and improvements of the NFIU framework it is ready made solution for NATO to fill the gap.

The alternative option could be that host nations will take over full preparation and the coordination role to facilitate deployment of the Allied forces. That will put additional burden and resource requirement for the receiving nations in the times when the primary focus is preparation for defence or even warfighting. It also could reduce the situational awareness in the NATO Commands and for the forces under deployment. Therefore, NFIUs are beneficial for the host nations by reducing the workload of national command structures and letting them to keep the focus on warfighting.
What adaption NFIUs require for the new role?

The outcome of the survey shows that all NFIUs implementing same wide range of tasks with few exceptions of additional duties. Moreover, most of the NFIU commanders answering the questionnaire indicated overlap of the tasks currently performed by NFIUs and feasible requirements of the future tasks for NATO adaptation (see Graph 1). Added duties of the Units include STRATCOM and occasional

involvement in support of Alliance assurance measures or enhanced vigilance activities in respective country or region. Some NFIU commanders have been noting that the role of NFIUs could even increase in the future due to the implementation of NATO NFM.

In general, currently performed and for the future adaptation required tasks are not different and could be divided in four main groups. Provide situational awareness, support operational and exercise planning, maintain information data base, and provide facilities to support NATO forward command elements or host nation.



a) Facilitate RSOM/deployment of the NATO/allied forces including hosting recce teams.

b) Provide comprehensive Situational Awareness /Understanding on respective HN for NATO Higher Command/Units

c) Maintain civilian and military network within HN and NATO commands for information exchange.

d) Maintain information data base for contingency and exercise planning.

e) Support operational and exercises planning of the HN and NATO

f) Provide continuous HNS advise and coordination for NATO Commands and Units

g) Support NATO forward deployed command elements.

h) Contribute to NATO STRATCOM and assurance.

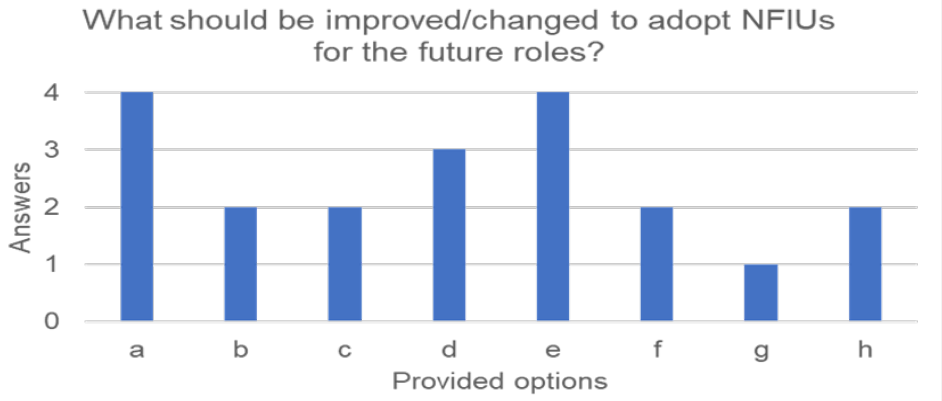
i) Provide Situational Awareness for HN on NATO processes and activities.

Graph 1: Comparison of survey answers for questions 3 and 4. Source: The NFIU Commanders questionnaire conducted by author.

Nevertheless, NFIU doctrinal documentation should be updated to meet NATO NFM terminology in future tasks assigned for NFIUs. Another question would be to update the name of the Unit for closer to meaning what the actual tasks are. Instead of the force integration unit it could be NATO Forward Coordination Unit.

To conclude, there is no requirement to change NFIUs tasks and roles. The requirement to facilitate deployment of Allied forces remains actual. Moreover, NATO NFM concept with 3 tiers approach increases necessity of contingency planning, support, and exercises for pre-assigned troops. The question may even rise on need to establish additional NFIU in Finland as a new member of NATO which is bordering with Russia and is potential destination for troop reinforcement.

The outcome of survey question five indicates the main shortfalls of the NFIUs and provides basis for further analysis of necessary development. The results are showing the most relevant improvement requirements. By summarising collected answers, the C2 and visibility are equally the most selected ones. Ability to operate outside of permanent location is the second highest pointed answer. Combination of training and exercise related replies provides the third area of concern (see Graph 2). Using the answers from survey four most relevant shortfalls were identified.



a) Change of the NFIU C2 from tactical level to operational level.

b) Improve NFIU Communications networks and functional systems.

c) Change the NFIU Structures (including crisis and war time purposes)

d) Improve NFIU deployability (Readiness to operate outside of permanent location)

e) Improve NFIUs visibility and engagement within NATO.

f) Improve NFIUs training programme (Training audience for NATO sponsored collective exercises)

g) Change NFIUs current mission and roles.

h) Improve NFIUs role in host nation exercises.

Graph 2: Survey answers for question 5. Source: The NFIU Commanders questionnaire conducted by author.

Following list is ranking shortfalls and requirements for improvement. Firstly, current NFIUs C2 arrangement has been seen not suitable for the NFIUs operating purpose. Being 'joint by nature' is by default linking NFIUs with operational level. Moreover, NFIUs structure and expertise is design to support all joint functions and operational domains with exception of space and cyber. Being linked to operational level does not mean that NFIUs are above tactical level units like Corps or Divisions, it is about subordination hierarchy of command and control to the operational level. Currently, subordination to the land tactical level command has hampered NFIUs coordination with maritime and air domain which has led them to bypass NFIUs.

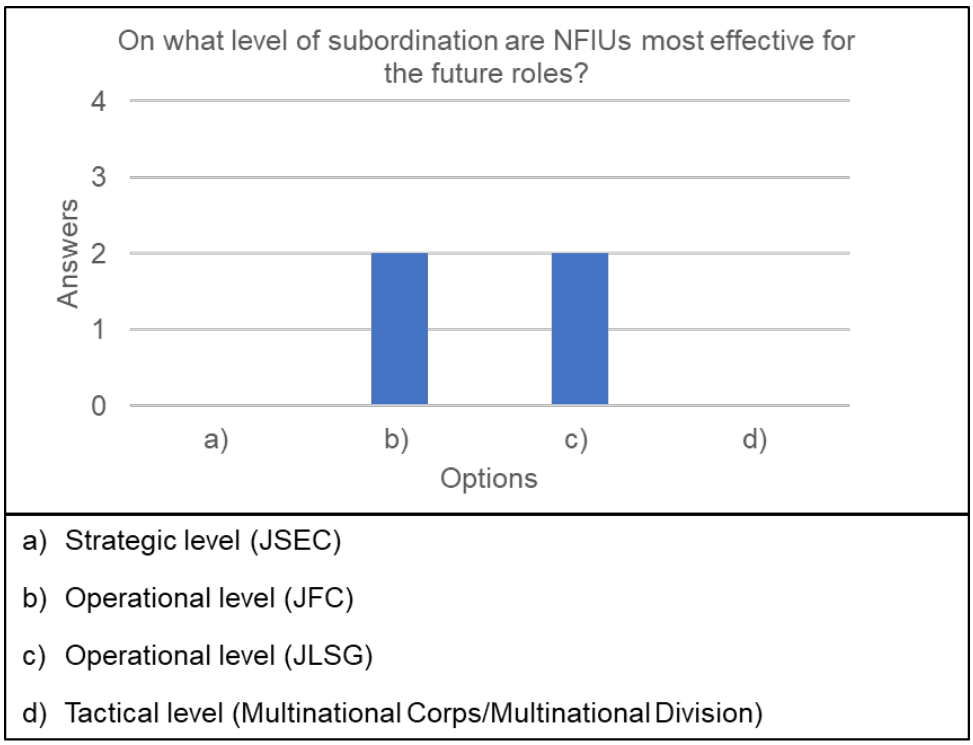
Secondly, although NFIUs are NATO Force Structure Units they are not recognized and visible in the overall NATO organisation. In the beginning when NFIUs were founded wide media coverage took place and Units were presented as NATO persistent presence in the Alliance eastern border area. Although, having an important

role in RAP concept as facilitator of the rapid deployment for VJTF after introduction eFP concept NFIUs have lost their visibility and role in assurance messaging. Moreover, even stronger signal of the low visibility and gap in the understanding, both in NATO and host nations, is fact that NFIUs are not represented in NATO doctrinal documentation with exception of the AJP-4.3 Allied Joint Doctrine for Host-Nation Support. (NATO AJP-4.3, 2021 p. 15)

Thirdly, currently NFIUs have access to command-and-control systems only from permanent dislocations. That is limiting very much the capability of the units to perform tasks from alternative locations or to send out liaison teams. Secure communication and information systems are key for NFIUs daily work. The access to the information, databases and networking is crucial to assure situational awareness and share information with the customers. Requirement to relocate unit differs from the country to country and is especially paramount for the Baltic states. Operational depth and distance from borders with actual threat is much shorter compared to other NFIU's locations. Relocation of unit becomes especially important in case of direct attack during the crisis or conflict.

Fourthly, the doctrinal gap regarding the NFIUs has created situation where the Units have been left out from the general NATO exercise cycle and occasionally in host nation exercises. In the years 2015 – 2016 NFIUs were involved in the JUMP-series exercises, which included also testing the concepts behind the NFIUs (SHAPE Public Affairs Office, 2015). In recent years it has been not systematic and as a result of that visibility of the NFIUs in the wider NATO organisation has diminished even more. Understanding of the units' capabilities is reduced and evolution of the NFIU framework has been marginal over the last years. Moreover, rotations of the eFP battlegroups have been institutionalized outside of the NFIUs scope due to the framework nations direct C2 arrangements with hosting country.

The outcome of the question 6 which is closely linked with analysis of the previous question showing clearly need for change of the NFIUs current C2 arrangements. All participants have suggested change in subordination from tactical level to the operational level. Only difference appears between selected choices of subordination between the Joint Force Command and to the Joint Logistics Support Group (see Graph 3).



Graph 3: Survey answers for question 6. Source: The NFIU Commanders questionnaire conducted by author.

Subordination to the operational level HQs will clearly provide better conditions for cross domain activities and improve information exchange. Moreover, linking with operational level provides flexibility which allows NFIUs to deliver support for all levels of operations and establish necessary network for maintaining situational awareness. Linking NFIUs with the joint commands will also enhance collective training and exercise opportunities. Moreover, the exercise scenarios on operational level often includes pre warfighting phases of conflict and deployment of the Allied forces. That is primary timeframe for NFIUs to facilitate and support deployment of the forces. Although, tactical level could also design exercises for pre warfighting phase their primary focus remains still to train HQs and troops for the war. Adding NFIUs as training audience to the NATO exercise programme will provide basis for lesson learned process, doctrinal development and significantly improve visibility of the units.

Summary

Russian aggressive actions since 2008 and attack against Ukraine in 2022 have significantly deteriorating the security of Europe. Moreover, it has challenged entire international rule-based order. As a response to that NATO has stated the Russian

Federation as direct military threat to Allies. To assure peace and security for Alliance members NATO started to improve its responsiveness and readiness. In 2014 introduced RAP was focussing on two main aspects – assurance and adaptation. NATOs responsiveness was enhanced by introducing VJTF concept which included NFIUs as NATOs persistent presence in eastern Allies with task to facilitate deployment of VJTF. While NATO was aiming to avoid escalation of the situation and was reactive in principle Russia continued its aggressive actions. NATOs response did not satisfy Baltic states and Poland and in 2016 Warsaw more credible posture of the eFP/tFP was introduced. For Baltic states eFP was important step forward for Alliance responsiveness, but consequently VJTF concept became secondary. The value of the NFIUs diminished and soon the relevance of the Unit from host nation perspective was questionable. In 2022 NATO introduced new Strategic Concept and development of the NFM and DDA with new 'family of plans'. This new concept and major adaptation of the NATO forces and command structure led to the need for the adaptation assessment of the NFIU concept.

Analysis of the strategic documents and the survey outcome shows that in perspective of the new doctrines and NATO 2022 Strategy current NFIUs roles and tasks are still relevant. NATO NFM will replace the current NRF, and pre-assigned forces will be linked to specific defence plans with assigned areas of the responsibility, but the deployment challenge will remain exist. Therefore, from NATO perspective NFIUs are important assets in facilitating and coordinating role to assure responsiveness of NFM. With new approach, adaptation, and improvements of the NFIUs it is ready made solution for NATO to fulfil the task. Moreover, Finland, as border country with Russia, has recently joined to NATO and therefore option to establish NFIU there could be also considered.

Current command and control arrangements of the NFIUs are not appropriate for the unit mission and purpose. Analysis of the concepts, NFIUs mission and tasks, and supported by survey showing several shortfalls on that area. Therefore, NFIUs, although being part of the NATO Force Structure, subordination should be directly to the operational level. That arrangement will clearly provide better conditions for cross domain activities and improve information exchange. Linking with operational level and exercising appropriate level of mission command provides NFIUs necessary flexibility in execution of its mission.

Shortfalls of unit level training and exercises for NFIUs are directly derived from inadequate C2 arrangement and lack of proper 'sponsorship' in NATO. Leaving NFIUs out from the NATO exercise programme has led to the situation where doctrinal development of the units is literally not existing and visibility of the units is diminished. Moreover, NFIUs have been left with no proper support for further development for crisis and war time capabilities. That is especially important in situation when NATO assessment of the strategic environment defines the Russia as the most significant and direct threat to Allies'. NFIUs situated in the NATO eastern border countries are remarkably more vulnerable position with no capability to operate from alternative location.

As conclusion, 'Whether and what adaptation NFIUs require in the new security situation after February 2022?', analysis of NATO Strategic documentation and the NFIU commanders' survey approves the relevance of NFIUs for the NATO NFM with the currently assigned functions. Most appropriate adaptation requirements of NFIUs are in the C2 arrangements, unit level training and in preparedness for crisis. NFIUs are also beneficial for the host nations by reducing the workload and letting them to focus on warfighting. NFIUs have to be adapted to the new 'prepare to defence mode' which includes ability to operate in a deployed mode from varied locations.

As an outcome of the analysis the following conclusions for decision makers can be made:

- NFIU should be adopted to support NFM with roles and tasks remain as these are stated currently. Doctrine should be adopted from facilitating NRF to the support of NFM and all Alliance forces.
- Subordination of the NFIUs should be changed to the operational level with proper mission command principles and flexibility for action.
- Unit level training of NFIUs should be improved by adding units to the NATO exercise programme as training audience.
- Survivability and sustainability of the Units should be improved with capability to operate from alternate locations.
- Utilizing NFIUs to assist assurance measures and enhanced vigilance activities.
- Assuring the manning and contributing nations support to units.
- Increase the visibility of the NFIUs within NATO.

- Considering the adaptation of the NFIUs name to the NATO Force Coordination Unit

Above listed suggestions are general conclusions based on outcome of the conducted analysis. Although there is substantial overlap in the tasks what NFIUs are currently performing, every unit has its specific conditions due to the location and role in hosting country. Therefore, keeping the conceptual foundation broad will allow units to adopt to the necessary local specifics.

Bibliography

Arnold, John-Michael. 2016. NATO's Readiness Action Plan: Strategic Benefits and Outstanding Challenges. *Strategic Studies Quarterly.* 2016, Vol. 10, 1, pp. 74-105.

Bauer, Rob. 2022. NATO. *The NATO Military Committee.* [Online] 19 May 2022. [Cited: 02 April 2023.] https://www.nato.int/cps/en/natohq/opinions_195246.htm?selectedLocale=en.

Botik, Martin and Mazel, Jan. 2022. NATO Force Integration Units: Are NFIUs a Valuable Element of NATO Deterrence and Defense Posture? *Vojenské Rozhledy č.* 2022, Vol. 4, pp. 71 - 80.

Estonian Foreign Intelligence Service. 2018. International Security and Estonia 2018. *Valisluureamet.* [Online] 2018. [Cited: 15 April 2023.] https://www.valisluureamet.ee/doc/raport/2018-en.pdf.

—. 2022. International Security and Estonia 2022. *Valisluureamet.* [Online] 2022. [Cited: 15 April 2023.] https://www.valisluureamet.ee/doc/raport/2022-en.pdf.

Fryc, Mariusz. 2016. From Wales to Warsaw and Beyond: NATO's Strategic Adaptation to the Russian Resurgence on Europe's Eastern Flank. *Connections.* 2016, Vol. 15, No. 4, pp. 45 - 65.

Joint Force Command Brunnsum. 2020. Joint Logistic Support Group Brunssum. [Online] 2020. [Cited: 07 April 2023.] https://jfcbs.nato.int/page5964943/2020/joint-logistic-support-group-brunssum-established.

Joint Force Command Brunssum. 2022. NATO Response Force (NRF) 2022. *Joint Force Command Brunssum.* [Online] 2022. [Cited: 02 April 2022.] https://jfcbs.nato.int/page5725819/nato-force-integration-units/nato-force-integration-units-fact-sheet.

Leuprecht, Christian. 2019. The enchanced Forward Presence: innovating NATO's deployement model for collective defence. *NATO Defence College.* [Online] October 2019. [Cited: 02 April 2023.] https://qspace.library.queensu.ca/bitstream/handle/1974/28816/PB22_19.pdf?sequence=1.

Luik, Jüri and Praks, Henrik. 2017. Boosting the Deterrent Effect of Allied Enchanced Forward Presence. *International Centre for Defence and Security.* [Online] May 2017. [Cited: 02 April 2023.] https://icds.ee/wp-content/uploads/2017/ICDS_Policy_Paper_Boosting_the_Deterrent_Effect_of_Allied_eFP.pdf.

Madrid Summit. 2022. NATO. *Madrid Summit Declaration.* [Online] 29 June 2022. [Cited: 02 April 2023.] https://www.nato.int/cps/en/natohq/official_texts_196951.htm.

Mercier, Denis. 2018. NATO's Adaptation in an Age of Complexity. *PRISM.* 2018, Vol. 7, No. 4, pp. 2-11.

NATO 2022 Strategic Concept. 2022. NATO 2022 Strategic Concept. *NATO.* [Online] June 2022. [Cited: 03 April 2023.] https://www.nato.int/strategic-concept/.

NATO AJP-01. 2023. *Allied Joint Doctrine, Edition F, Version 1.* s.l. : NATO Standardization Office (NSO), 2023.

NATO AJP-4.3. 2021. *Allied Joint Doctrine for Host-Naition Support.* s.l. : NATO Sstandardization Office (NSO), 2021.

NATO Fact Sheet JSEC. 2021. Joint Support Enabling Command. [Online] May 2021. [Cited: 07 April 2023.] https://jsec.nato.int.

NATO Fact Sheet NFIU. 2015. NATO Force Integration Unit. *NATO.* [Online] September 2015. [Cited: 02 April 2023.] https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2015_09/20150901_150901-factsheet-nfiu_en.pdf.

NATO New Force Model. 2022. NATO New Force Model. *NATO.* [Online] 2022. [Cited: 02 April 2023.] https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/220629-infographic-new-nato-force-model.pdf.

NATO Readiness Action Plan. 2016. NATO Readiness Action Plan. *NATO.* [Online] Public Diplomacy Division, July 2016. [Cited: 02 April 2023.] https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_07/20160627_1607-factsheet-rap-en.pdf.

NATO Strategic Concept. 2010. *NATO Strategic Concept 2010.* s.l. : NATO, 2010.

SHAPE Fact Sheet. NATO Force Integration Units (NFIU). *SHAPE.* [Online] [Cited: 01 April 2023.] https://shape.nato.int/operations/nato-force-integration-units.

SHAPE Public Affairs Office. 2015. NATO 'Spearhead' Force deploys for first time, Exercise Noble Jump underway. *SHAPE Public Affairs Office.* [Online] SHAPE , 15 June 2015. [Cited: 02 April 2023.] https://www.nato.int/cps/en/natohq/news_120512.htm.

Stoicescu, Kalev and Praks, Henrik. 2016. Strateegilise tasakaalu tugevdamine Läänemere piirkonnas. *ICDS.* [Online] March 2016. [Cited: 10 March 2023.] https://icds.ee/wp-content/uploads/2016/Kalev_Stoicescu__Henrik_Praks_-_Strateegilise_tasakaalu_tugevdamine_Laanemere_piirkonnas.pdf.

Stoltenberg, Jens. 2022. Reuters. *NATO to boost troops on high alert to over 300,000 -Stoltenberg.* [Online] 27 June 2022. [Cited: 02 April 2023.] https://www.reuters.com/world/europe/nato-massively-increase-high-readiness-forces-300000-stoltenberg-2022-06-27/.

Wales Summit. 2014. *Wales Summit Declaration.* s.l. : NATO, 2014.

> I ask you one thing. Just give Europe to Russia. The U.S. is not in Europe. Europe should be the business of Europeans. Russia is half European and half Asian. Boris Yeltsin to Bill Clinton in 1999 (Clinton Digital Libraries, 1999).

Introduction.

For Estonia, all aspects of its security are existential due to its size, location, and threat from Russia. Therefore, security-related documents and activities must be adequate, measurable, understandable and connected from the national-strategic level to the military-tactical.

In 1999, then Major General Ants Laaneots and the Chief of Staff of the Estonian Defence Forces (EDF) claimed that EDF, as is, is deterring the adversary (Laaneots, 1999). Similarly, Estonian National Security Concept (NSC) from 2023 (Estonian Government, 2023) emphasises that the purpose of the military defence `… is to prevent military threats and, if necessary, to successfully defend the country and win the war` and `… to deter any potential adversary from launching a military aggression, Estonia adopts a forward defence posture, which combines national military defence capability and collective defence.` These two examples and conducted research (Veebel, et al., 2018) highlight the importance of deterrence in Estonian strategic military thinking at different times. Paradoxically, the rhetoric in the pre-NATO era was much more ambitious than what can be witnessed in the current National Security Concept. However, while in a different capacity, deterrence still holds a relevant position in the Estonian contemporary security approach. Even a cursory, empirical look at deterrence as an Estonian military strategy questions its validity. The following is not trying to find out why but instead offers suggestions of why not.

This research paper claims that deterrence as a military strategy is not feasible for Estonia when countering the Russian conventional military threat, neither from a unilateral nor from NATO`s collective defence perspective. Instead, Estonia must focus on its defence.

Given research does not question the credibility and effectiveness of NATO`s conventional and nuclear deterrence. However, these topics are outside this paper`s

focus due to the need to look deeper into deterrence from Estonia`s perspective. Prudence alone dictates the need for Estonia, relying on its security on NATO and its own military force, to assess how to counter the Russian military threat unilaterally. As the last few years, mainly through COVID-19 and Russian expanded aggression against Ukraine, have demonstrated, the events in the world have become less predictable and more concerning from a security perspective. Political disagreements, such as unwillingness to contribute to independent and collective military defence, inside NATO or a military conflict somewhere else in the world drawing resources and attention, are just two examples of potential situations where Estonia, at least temporarily, cannot fully count on its NATO allies.

This paper is divided into three parts. First, it will provide an overview of deterrence from a small country`s perspective; second, it will describe why deterrence is not feasible for Estonia; and the third part will focus on a summary and recommendations.

Deterrence from a small country`s perspective.

This paper defines deterrence as `the process of convincing a potential adversary that the costs of an action outweigh the benefits` (Jervis, 1976). This definition was chosen among many due to its simplicity, clarity and approach to deterrence as a process, unlike NATO, which approaches deterrence as part of its strategy as well as a task (NATO, 2022) (NATO, 2022).

Deterrence, the predominant framework of security during the Cold War, came under criticism with the collapse of the Soviet Union (Paul, 2009). With one of the two nuclear superpowers gone, it was considered that deterrence might not have any value in it. However, the emergence of rogue states and terrorist groups after the end of the Cold War and the terrorist attacks of 9/11 on US soil revitalised the importance of deterrence (Jervis, 2009). After Russia re-attacked Ukraine in 2022, deterrence also returned to the conventional realm, as can be witnessed in NATO’s Strategic concept of 2022 (NATO, 2022). Specifically, the mentioned concept brings deterrence up as one of NATO`s core tasks – Deterrence and Defence (NATO, 2022). This short description of deterrence history highlights two relevant points: (1) deterrence has been around since the end of the Second World War, with different focus and aims (Morgan, 2012), and (2) most deterrence-related theories and practices have been and are focusing on big powers, most notably on the US, and their options of why and how to deter. Thus, the

literature on how a small state could deter a more significant state from conventional military attack[1] is proportionally thin. However, there are enough thoughts to illuminate how a weaker state could deter a stronger one.

Layered deterrence.

Jonatan Vseviov, the former Estonian undersecretary of the Ministry of Defence and ambassador to the US, has studied how to construct deterrence in the Baltic States (Vseviov, 2021). In his study, Vseviov presents a three-layered approach to how to deter Russia in the Baltic region credibly:

1) Use of the Baltic states' forces
2) Use of in-place NATO forces
3) Use of NATO reinforcements

The author believes these layers are interconnected since the Baltic states could not successfully counter the Russian conventional attack (Vseviov, 2021). Despite that, this paper will only review the first layer focusing on utilizing the Baltic states' forces to construct deterrence. The reasons for such separation are (1) the scope of the current paper, (2) the potential benefit of given recommendations without follow-up steps, (3) Estonian substantially increased military spending and capabilities since 2022 (Estonian Ministry of Defence, 2022), and (4) Russian Military`s underwhelming performance[2] in Ukraine (Dalsjö, et al., 2022).

Vseviov suggests the following steps for each Baltic state to bolster their deterrence:

1) Authority to engage delegated to the lowest possible unit level.
2) Units spread in all regions of the country and in high readiness.
3) Quick response time to deny the adversary to accomplish fait accompli.
4) Capability to react decisively would force the adversary to commit conventional forces and therefore exclude the possibility of plausible deniability.
5) Ability to operate as long as it takes for NATO forces to arrive (Vseviov, 2021).

[1] Based on described limitation, the sources dealing with how to deter cyber, hybrid and similar non-conventional means will not be covered. While such means could indirectly contribute to deterring the adversary conventionally, they are outside of the scope of this paper.

[2] It is important to note that the assertion of Estonia's ability to confront Russia effectively cannot be made. Nevertheless, a critical evaluation of the Russian Military's status is imperative, as the assumptions employed in several wargames and analyses, based on which most pre-2022 assessments rely, are flawed and should be re-assessed.

Vseviov also covers the importance and challenges of communicating deterrence to Russia and acknowledges the potential shortfalls in sending and receiving ends (Vseviov, 2021). The author, however, does not explain based on what criteria he came to these recommendations and, most importantly, how such steps would increase the deterrence effect, separately in each layer or combined.

Unconventional deterrence.

Several authors have proposed unconventional warfare or utilising unconventional deterrence as a mechanism allowing small state/weak actor to deter bigger/stronger (Arreguin-Toft, 2009) (Salum, 2018) (Rekasius, 2005).

Salum suggests that small states lacking sufficient resources to counter the adversary conventionally might use their resources to build up their unconventional warfare capabilities either to (1) reinforce the conventional defence plan, (2) replace the conventional plan, or (3) deter a possible adversary, through approaching the unconventional warfare as a small state national security strategy (Salum, 2018).

According to Arreguin-Toft, in asymmetric conflicts he analysed in fifty-year periods from 1800 – 1999, the percentage of weaker actors‘ victories increased gradually from 11,8 per cent in 1800-1849 to 51,2 per cent from 1950 to 1999 (Arreguin-Toft, 2009). The author highlights four elements needed for the weaker side to win: `… social support, sanctuary …, an idea capable of making self-sacrifice seem both necessary and noble …, and a strategy capable of tying all three advantages into a single effort` (Arreguin-Toft, 2009). The author acknowledges that unconventional deterrence is more likely to succeed against Western countries with lesser tolerance for their casualties (Arreguin-Toft, 2009).

Another author, Rekasius, has proposed that unconventional deterrence is a method to overcome the imbalance of military power using guerilla warfare as a denial strategy and terrorism on the attacker`s soil as a punishment strategy (Rekasius, 2005). Two case studies provided by the author, the Vietnam War of 1964 – 1973 and the Afghanistan War of 1979 – 1989, are convincing examples of how the weaker side denied the stronger opponent‘s goals. However, it provides a little insight into how the weaker side, using unconventional deterrence, might succeed in preventing conflict.

One part of the solution offered by the writer – terror acts on opponents‘ territory – can be ruled out in the case of Estonia for legal and moral reasons.

Unconventional warfare has a substantial part in EDF capabilities and responses to potential aggression (EDF, 2022) and similarly, armed resistance as an activity is mentioned in EDF Organisation Act, the law regulating EDF status and tasks (Riigikogu (Estonian Parliament), 2023). Unconventional warfare plays a notable role in Estonian defence; however, it is doubtful how unconventional ways and means might deter Russian conventional attack. Relying on unconventional warfare/deterrence only would, by default, mean prolonged conflict and loss of territory, which could lead to the victory Estonia as a state cannot afford.

The examples of the Afghanistan War of 1979 – 1989 and the First Chechen Campaign of 1994 – 1996 clearly demonstrate that smaller, weaker, unconventional actors can defeat Russia. Still, there are no known cases of Russia being deterred by unconventional warfare or deterrence. As Javier has noted, while properly employed resistance and guerilla activities can influence the war‘s outcome substantially, it is questionable how such activities contribute to deterrence (Javier, 2023). Unconventional deterrence value is especially unclear when dealing with an adversary such as Russia, whose primary threat is not from its conventional capabilities but from brutality and risk acceptance accompanying the conduct of Russian warfare (Dalsjö, et al., 2022). From the Estonian independent defence perspective, unconventional warfare is a supporting effort and/or contingency but not a main effort when countering Russian conventional attack.

No deterrence.

Former supreme allied commander of NATO, retired U.S. Navy admiral James Stavridis has commented on a potential conventional military attack in NATO‘s eastern flank following: `While over the long term Russia would find itself overmatched by NATO (which outspends Russia on military activity by approximately 10-to-1), the short-term outcome could be a NATO capital or two in Russian hands` (Stavridis, 2019). This statement suggests little faith in the 2019-time deterrence capabilities of the NATO and NATO countries, including Estonia. A similar, if not more adverse, assessment has been provided by Halas, who suggests that deterrence does not work in the Baltics (Halas, 2019). According to Halas, dysfunctional conventional deterrence

is not a problem since Russia has no intentions to attack Baltic states conventionally (at the time of writing). Therefore, the focus should be on deterring Russia sub-conventionally. Halas also claims that no matter what the actions from the Estonian, Latvian and Lithuanian sides to bolster their security, it will not lead to deterred Russia (Halas, 2019).

From an Estonian perspective, we can divide sources that deal with small state options for deterring larger ones into three categories:

1) Increase the deterrence value by increasing its defence capabilities and relying on NATO allies‘ forces, capabilities, and cooperation.
2) Use of unconventional warfare or unconventional deterrence to deter Russia.
3) Some claim that Estonia cannot militarily deter Russia from a conventional attack.

No source claimed that (1) increasing Estonian military capabilities would deter Russian conventional attack or (2) increasing only Estonian military capabilities would increase NATO deterrence regarding Russian conventional attack. Most importantly, there was no clear argumentation in articles advocating for small state deterrence capabilities about how and why specific policies or activities would affect the deterrent value and how to measure it. The next part of the paper focuses on why Estonia should refrain from relying on deterrence as a strategy to counter the conventional Russian threat.

Reasons for not using deterrence in the case of Estonia.

According to Paul, for deterrence to be effective, it must base on three principles:

1. An actor intending to deter must possess the necessary capability.
2. Credibility of threat.
3. Ability to communicate the threat to the adversary (Paul, 2009).

Necessary capability.

One of the critical issues for Estonia regarding its deterrence posture towards Russia is the general disproportionateness of power (Praks, 2018). While this statement holds from perspectives of the size of the country, population, industrial capability and so forth, this paper focuses on conventional military capability and its imbalance. The question immediately arises – how much and what kind of military capability should

Estonia possess to deter a Russian conventional military attack? In other words, what are the aspects what Russian leadership would fear, and how much of it should Estonia have? Veebel has suggested that Baltic states should focus on `high-readiness, professionalism and decisiveness of the military forces` since these are the strategic strengths Russia values most and might view as a potential deterrent when assessing other countries (Veebel, et al., 2019). However, the Russian war in Ukraine from 2022 has proven that Russia itself does not uphold the strengths valued – its troops have not demonstrated high readiness, professionalism or decisiveness. This does not, however, make the Russian threat smaller, perhaps less advanced, or as Chief of EDF, General Herem has said:

> We have painted a picture of the Russian war machine that's dumb, sports low morale and is easy to overcome. But this `bunch of bandits` is killing hundreds of people and leveling cities every day, no matter how big of a shambles it looks (Herem, 2022).

Contrary to Veebel‘s one recommendation, increased professionalism, Estonia, due to the events of the Russian war in Ukraine from 2022, decided to increase the EDF wartime structure by 10 000 to 37 000 by 2024 by adding additional reservists (Uudeberg, 2022). According to the rule where the attacker must have 3 to 1 superiority over the defender in conventional battle (Mearsheimer, 1988), one could argue that Russia would need around 100 000 troops to attack Estonia successfully conventionally. This formula, while potentially providing some scale of forces required, is, on the other hand, deceptive. First, this ratio would not provide any basis for deterring Russia but only for defending Estonia from Russia. Second, these numbers would not consider the Russian naval and aerial superiority in the region and simultaneously, such calculus would not account for EDF‘s recent procurements, such as long-range fires, different anti-tank and artillery weapons, mid- and short-range air defense systems and loitering munition (Laanet, 2022). Third, it is crucial to consider nonmaterial yet critical variables, such as how forces are used, their motivation, training and skills. As one expert has stated, `In fact, analyses considering materiel alone may be little better than blind guesses` (Biddle, 2004).

Questions raised in this overview of the necessary capability to deter – how much is enough and – how to measure it are beyond the scope and length of this paper. It can be argued that mathematically and conceptually, it is much more realistic to determine how much and what is required to defend than deter. Still, the required deterrence

capability must be known/visible to the adversary. When comparing conventional and nuclear deterrence, an expert has stated that showing capability is necessary for conventional deterrence, whereas nuclear deterrence mostly depends on the determination to use it (Freedman, 2004). In addition to possessing and demonstrating the capability, one must ensure the threat's credibility.

The credibility of the threat.

Morgan suggests that threats issued are less effective than in the Cold War era, and it is challenging to make the threats credible (Morgan, 2012). Contrary to this, there is no reason to doubt the Estonian threat's credibility. The Constitution of the Republic of Estonia states that every citizen of Estonia must remain faithful to the constitutional order and protect Estonia's independence. If there are no other options to counteract an attempt to alter Estonia's constitutional order, every citizen can resist such an attempt independently (Riigikogu (Estonian Parliament), 1992). The poll conducted in the spring of 2022 found that:

1) 78 % of residents trust EDF,
2) 81 % of the population considered that armed response to respond to an armed attack is certainly or rather necessary,
3) 60 % of residents definitely or somewhat agreed to take part in defence of Estonia, by their abilities,
4) the confidence in Estonia's ability to defend itself until allied assistance arrives has reached its highest level in the past five years, with 60% of people holding this belief,
5) over 80 % of people support the conscription service (Eesti Uuringukeskus OÜ (Estonian Research Centre), 2022).

Additionally, the statements by Estonian politicians and military leaders leave no doubt in Estonian resolve to counter the conventional Russian aggression. Also, the increased intensity and size of regular and snap military exercises and increased military spending are proof of commitment to defend Estonia. To summarise – Estonia is demonstrating its credibility to threaten Russia against aggression in many ways. It means legal preparedness, sizeable popular support, statements by its political and military leadership and conduct of military exercises in conjunction with improving military capabilities. According to a security expert, the concern may not lie in the

legitimacy of a threat but rather in the severity of the threat (Press, 2005). The threat‘s seriousness also depends on how it is communicated and received.

Ability to communicate the threat.

Veebel suggests that deterring Russia is questionable due to the reasons tied to communication (Veebel, 2021). First, there are linguistic challenges – there is no direct translation of deterrence into the Russian language; second, it has a significant cultural impact characterised by a tendency towards condescension and control; and third, Russian leadership and population are unanimous in their assessment that Russia is not and will not be deterred (Veebel, 2021). This example highlights the importance and challenge of tailoring the message. According to Adamsky, it is challenging for the sender of the deterrence message to ensure that the signal is received and interpreted the way it was initially meant (Adamsky, 2017). Paradoxically, similar issues appear to be relevant on the Russian side. As Bruusgaard states, it is questionable `… whether the adversary will understand the message of deterrence the way the Russian concept prescribes it` (Bruusgaard, 2016). Adamsky argues similarly that Russia lacks a system of evaluating the effectiveness of its deterrence towards the adversary (Adamsky, 2017). Based on these last two statements, it is logical to deduct with a high probability that Russia lacks the process of evaluating the adversaries‘ deterrence-related messages and activities as well. Military-related signals are incredibly challenging and even amplified psychologically during the crisis (Freedman, 2004).

In Russia, the message‘s recipient is its president, Vladimir Putin. According to several sources, from the beginning of the COVID-19 pandemic, Putin has become increasingly isolated from the outside world and receives information only from a handful of people close to him (Kinetz, 2023) (Shull, 2022). Putin‘s isolation will add another filter or filters to an already complex situation of sending, receiving, forwarding and interpreting the messages. Paradoxically, even if Putin received the threat message and interpreted it the way it was initially meant and agreed with the message, it does not automatically translate into agreement. In other words, the person to be deterred might decide otherwise, even if everything is mathematically and logically aligned (Gray, 2007). The reasons for such `refusal to be deterred` can be various – above-average risk acceptance, mental illness or other political considerations, to name a few. Since the messaging must focus on the decision-maker, Putin, in this

case, it follows that if Putin‘s follower‘s era is similarly hostile to Estonia, but the follower‘s (and his close circle‘s) background and personality are different from Putin‘s, then everything in described deterrence machinery must be reassessed and possibly rearranged, what could be time and resources heavy.

To summarise – critical elements for deterrence to be effective are sufficient military capability, credible threat and ability to communicate the threat. Determining the exact nature and size of a convincing military capability required to deter is challenging. Additionally, no proven formula or process warrants the threat‘s credibility. Finally, the message of deterrence threat must be communicated and received to avoid getting lost in translation and interpretation. This all raises a question – how does one measure the success of deterrence?

The unit of measure for (un)successful deterrence.

It is telling that not a single source in this paper used to this point has yet to offer any solutions for measuring the success of the deterrence measures/methods proposed by the authors. No percentage, no more/less likely/probable or anything else regarding how the ways and means offered might influence the outcome. However, there have been numerous attempts to explain the success or failure of deterrence.

Rand Corporation, for example, has conducted a thorough analysis of several U.S-related general deterrence cases from 1945 to the present (Mazarr, et al., 2018). This research, however, raised some questions. For example, the authors‘ analysis demonstrated that deterrence did not fail when the aggressor‘s motivation was low or that deterrence did not fail due to the obvious U.S. and its allies‘ advantage in the local balance of power (Mazarr, et al., 2018). Given insights are not helpful not only in the case of Estonia but in general when looking for ways and means to boost deterrence. Another study focused on determinants of successful or failed deterrence cases from 1900 to 1980 (Huth, et al., 1984). The findings of this article are insightful, such as the claim that the past behavior of the defender regarding deterrence played no role in the outcome of the case observed (Huth, et al., 1984). What makes this analysis and its conclusions less valuable for Estonia is that it focuses on immediate deterrence. The challenge in general with this and similar studies is that since every case is unique in place, time and political settings, it is hard to conclude what applies to other cases.

The Estonia-specific challenge of case studies is similar to the problem of overall deterrence literature from an Estonian perspective – its focus does not apply to Estonian requirements and parameters.

Gray is among the writers acknowledging the complexity of measuring the success of deterrence: `If 50 missiles are believed to be quite deterring, it does not follow that 100 missiles are twice as deterring` (Gray, 2007). Thus, deterrence, its utility and success probabilities are not linear and, according to Gray, cannot be calculated mathematically due to the human factor (Gray, 2007). Since every deterrence case is different and there is no formula for how to calculate its outcome, it is perhaps best to follow the recommendation Freedman gave to practitioners confronted by the situation they are facing: `… the best advice must be to draw on some careful empirical work on the situation at hand as much as on any work of theory. Even then, there is no guarantee of success` (Freedman, 2004).

Estonian practitioners have taken this advice offered by Freedman and crafted their response accordingly. In the spring of 2022, Estonian Prime Minister Kaja Kallas stated that in Estonia, NATO should change from deterrence to defence (Kallas, 2022). Such an argument might be interpreted as a lack of confidence both in Estonian independent as well as NATO‘s general force posture‘s deterrent value in Estonia. On the other hand, an author has stated that deterrence `… is one of the core strategic functions of any defence organisation` (Oonincx, 2020). There are, however, no absolutes, especially when a matter at hand, such as deterrence, can be viewed as a matter of faith (Halas, 2019). Chief of EDF, General Herem, has indicated his lack of confidence in deterrence, saying `I no longer have faith in deterrence. Invading Ukraine was clearly insane, yet they still did it. I only believe one thing – that we need to be ready to dispatch as many of the enemy as cross the border` (Herem, 2022). This blunt statement from General Herem does not demonstrate a loss of faith in deterrence in general but rather a disbelief in the applicability of deterrence in a current, specific situation (Herem, 2023). Also, this message demonstrates the shift from deterrence to defence. This raises the question – can these two co-exist?

Deterrence and/or defence?

Estonian National Security concept states that the purpose of military defence is to deter military threats, and should this fail, then `successfully defend the country and

win the war` (Estonian Government, 2023). This statement suggests that deterrence and defence are sequential, linear and escalatory steps – if one fails, the other comes to play. Or in other words, defence is the contingency plan in case of deterrence failure. Deterrence is reactive in nature and gives the initiative to the enemy (Gray, 2007) and, therefore, might negatively impact defence readiness and war outcome from an Estonian perspective. Snyder has taken it even further and claimed that deterrence and defence as concepts are different and what deters might not defend and vice versa (Snyder, 2015). Another expert has come to similar conclusions. Posen categorised military doctrines as offensive, defensive or deterrent (Posen, 1984). According to the author, the military forces[3] designed to deter become specialised in punishment and have very limited defensive capability (Posen, 1984). To summarise – the use of deterrence might delay the defence, what deters might not defend, and forces designed to deter might not be capable of defending.

Other issues that arise when discussing deterrence are the meanings behind the words. Estonian National Security Concept mentions deterrence (Estonian Government, 2023). This author's interpretation of deterrence required by Estonia to deter Russian conventional military attack, based on explanations provided by Freedman, is strategic general (threat is not immediate) broad (to deter war, not specific military activity) conventional (as opposed to nuclear) extended (involves NATO) deterrence by denial[4] (deny enemy strategic options) (Freedman, 2004). Such formulation strongly indicates a need for a tailored, environment and enemy-specific approach. This author is unaware of the existence of the `Estonian deterrence implementation plan` – who (including NATO allies), what, when, where, why and how this impacts the adversary. If such a plan exists, then at least parts of it should be made public/available since deterrence works only if the adversary is aware of such intentions to a necessary extent.

Summary and recommendations.

Deterrence has been and still is central in Estonian security documents. However, the deterrence-related literature could be of more help to Estonia since most sources focus

[3] One example provided by Posen of the military forces designed to deter the enemy (through punishment) conventionally was Switzerland (Posen, 1984). The Swiss defence model, however, does not apply to Estonia due to the differences in geography and the intended way of fight.
[4] Another option is deterrence through punishment, but due to the lack of sufficient depth in Estonia, it is not realistic.

on big states, and the Estonian case is small and specific. Additionally, authors who concentrate on small state/unconventional deterrence suggest deterrence through punishment as a strategy, which, in the case of Estonia, countering Russian conventional attack is not a sufficient option. Moreover, no article had measurable or historically backed reasoning as to why a certain way or mean, if implemented, would increase the deterrence posture.

For deterrence to be effective, one must possess the required capability, credible threat and ways and means to communicate the threat to the adversary. To operationalise all these requirements, separately and in concert, is challenging. There are no rules of thumb or general formulas; ultimately, it is based on psychology – trying to estimate what deters the decision–maker and how to make it work.

Deterrence is not measurable, not predictable with a sufficient degree of certainty and subjective approach, a matter of faith. Additionally, it is challenging to see a clear, deterrence-related line of connected dots in Estonia, from the strategic level to the tactical, from strategy and policies to actions. Furthermore, even if the deterrence architecture was in place, it is questionable what the strategic utility of deterrence would be from an Estonian perspective when countering Russian conventional military attack.

While deterrence and defence are not mutually exclusive, there is a possibility of deterrence delaying the defence and a threat of reducing or diminishing defence capabilities by focusing on deterrence.

This paper recommends acknowledging that deterrence as a military strategy is not feasible for Estonia when countering the Russian conventional military threat, neither from a unilateral nor from NATO‘s collective defence perspective. Thus, all related documents from National Security Concept and below should be rephrased accordingly. What follows is that for the defence of Estonia, EDF must focus on defensive military doctrine only. Finally, a comparable study could be conducted in similar small states, such as Latvia and Lithuania, to explore the similarities and differences regarding the approach to deterrence and potential recommendations for the way forward.

Bibliography

Adamsky, Dmitry. 2017. From Moscow with coercion: Russian deterrence theory and strategic culture. *Journal of Strategic Studies.* 2017, Vol. 41, 1-2.

Arreguin-Toft, Ivan. 2009. Unconventional Deterrence How the Weak Deter Strong. [book auth.] Paul T. V., Morgan M. Patrick and Wirtz J. James. *Complex Deterrence Strategy in the Global Age.* Chicago and London : The University of Chicago Press, 2009.

Biddle, Stephen. 2004. *Military Power Explaining Victory and Defeat in Modern Battle.* Princeton and Oxford : Princeton University Press, 2004. 0-691-11645-8.

Bruusgaard, Kristine Ven. 2016. Russian Strategic Deterrence. *Survival.* 2016, Vol. 58, 4.

Clinton Digital Libraries. 1999. *Declassified Documents Concerning Russian President Boris Yeltsin.* Washington DC : s.n., 1999.

Dalsjö, Robert, Jonsson, Michael and Norberg, Johan. 2022. A Brutal Examination: Russian Military Capability in Light of the Ukraine War. *Survival Global Politics and Strategy.* 64, 2022, Vol. 3.

EDF. 2022. EDF Special Operations Forces. *https://mil.ee/en/landforces/special-operations/.* [Online] EDF, August 5, 2022. [Cited: April 01, 2023.]

Eesti Uuringukeskus OÜ (Estonian Research Centre). 2022. *Public opinion on national defence 2022.* Tallinn : Estonian Ministry of Defence, 2022.

Estonian Government. 2023. *Estonian National Security Concept.* Tallinn : s.n., 2023.

Estonian Ministry of Defence. 2022. Estonian Military Defence 2026. *Estonian Military Defence 2026.* [Online] Estonian Ministry of Defence, 2022. [Cited: April 06, 2023.] https://www.kaitseministeerium.ee/riigikaitse2026/eng/.

Freedman, Lawrence. 2004. *Deterrence.* Cambridge : Polity Press, 2004. 978-0-7456-3112-7.

Gray, Colin S. 2007. Deterrence in the 21st century. *Comparative Strategy.* 2007, Vol. 19, 3.

Halas, Matus. 2019. Proving a negative: why deterrence does not work in the Baltics. *European Security.* 2019, Vol. 28, 4.

Herem, Martin. 2022. EDF commander: I no longer believe in deterrence. *ERR News (Estonian Public Broadcasting).* [Online] ERR (Estonian Public Broadcasting), June 01, 2022. [Cited: April 5, 2023.] https://news.err.ee/1608615991/edf-commander-i-no-longer-believe-in-deterrence.

—. 2023. *Interview to clarify deterrence related statements.* April 13, 2023.

Huth, Paul and Russett, Bruce. 1984. What Makes Deterrence Work? Cases from 1900 to 1980. *World Politics.* 1984, Vol. 36, 4.

Javier, Erick Nielson C. 2023. *Alternative Options to Strengthen Small State Deterrence in the Face of New Great Power Competition.* Hague : The Hague Centre for Strategic Studies, 2023.

Jervis, Robert. 2009. Deterrence, Rogue States, and the U.S. Policy. [book auth.] Paul T.V., Morgan M. Patrick and Wirtz J. James. *Complex Deterrence Strategy in the Global Age.* Chicago and London : The University of Chicago Press, 2009.

—. 1976. *Perception and misperception in international politics.* Princeton NJ : Princeton University Press, 1976.

Kallas, Kaja. 2022. PM: NATO proposals for ramping up defense not enough for Estonia. *ERR News (Public Broadcasting) .* [Online] Public Broadcasting, May 12, 2022. [Cited: April 01, 2023.] https://news.err.ee/1608594982/pm-nato-proposals-for-ramping-up-defense-not-enough-for-estonia.

Kinetz, Erika. 2023. 'He's a war criminal': Elite Putin security officer defects. *AP News.* [Online] Associated Press, April 5, 2023. [Cited: April 7, 2023.] https://apnews.com/article/russia-putin-defector-war-crimes-khodorkovsky-karakulov-dossier-845421fe06ed9cfa1962ad4f98a2e413.

Laaneots, Ants. 1999. The Estonian Defence Forces - 2000. *Baltic Defence Review.* 1999, Vol. 1.

Laanet, Kalle. 2022. New €3.8-billion defense spending plan for 2023-2026 unveiled. *ERR News (National Broadcasting).* [Online] ERR (National Broadcasting), May 20, 2022. [Cited: April 5, 2023.] https://news.err.ee/1608604033/new-3-8-billion-defense-spending-plan-for-2023-2026-unveiled.

Mazarr, Michael J, et al. 2018. *What Deters and Why Exploring Requirements for Effective Deterrence of Interstate Aggression.* Santa Monica, CA : RAND Corporation, 2018. 978-1-9774-0064-2.

Mearsheimer, John J. 1988. Numbers, Strategy, and the European Balance. *International Security.* 1988, Vol. 12, 4.

Morgan, Patrick M. 2012. The State of Deterrence in International Politics Today. *Contemporary Security Policy.* 33, 2012, Vol. 1.

NATO. 2022. Deterrence and defence. *NATO website.* [Online] NATO, September 12, 2022. [Cited: April 19, 2023.] https://www.nato.int/cps/en/natohq/topics_133127.htm#:~:text=Deterrence%20is%20a%20core%20element,and%20the%20rule%20of%20law..

NATO, Summit. 2022. NATO Strategic Concept 2022. *NATO Strategic Concept 2022.* 2022 : NATO, 2022.

Oonincx, Patrick. 2020. Foreword. [book auth.] Frans Osinga and Time Sweijs. *NL ARMS Netherlands Annual Review of Military Studies 2020 Deterrence in the 21st Century—Insights from Theory and Practice.* Hague : Asser Press, 2020.

Paul, T.V. 2009. Complex Deterrence An Introduction. [book auth.] Paul T.V., Morgan M. Patrick and Wirtz J. James. *Complex Deterrence Strategy in the Global Age.* Chicago and London : The University of Chicago Press, 2009.

Posen, Barry P. 1984. *The Sources of Military Doctrine France, Britain, and Germany Between the World Wars.* Ithaca and London : Cornell University Press, 1984. 978-0-8014-9427-7.

Praks, Henrik. 2018. Estonia`s approach to deterrence Combining central and extended deterrence. [book auth.] Nora Vanaga and Tom Rostoks. *Deterring Russia in Europe : Defence Strategies for Neighbouring States.* s.l. : Taylor & Francis Group, 2018.

Press, Daryl G. 2005. *Calculating Credibility How Leaders Assess Military Threats.* Ithaca and London : Cornell University Press, 2005. 978-0-8014-7415-6.

Rekasius, Mindaugas. 2005. Unconventional Deterrence Strategy. Monterey, CA : Naval Postgraduate School, 2005.

Riigikogu (Estonian Parliament). 2023. Estonian Defence Forces Organisation Act. s.l. : Riigikogu (Estonian Parliament), 2023.

—. 1992. The Constitution of the Republic of Estonia. 1992.

Salum, Karl. 2018. Small State UW Doctrine: Feasibility and Application . [book auth.] Kevin D Stringer and Napier Glennis F. *Resistance Views Essays on Unconventional Warfare and Small State Resistance Tartu Resistance Seminar.* MacDill, FL : Joint Special Operations University, 2018.

Shull, Abbie. 2022. Putin has become so isolated during the pandemic that he no longer meets friends for 'drinks and barbecues,' a Russian journalist said. *Business Insider.* [Online] Business Insider, March 11, 2022. [Cited: April 04, 2023.] https://www.businessinsider.com/russian-journalist-putin-isolated-during-pandemic-2022-3.

Snyder, Glenn H. 2015. *Deterrence and defense.* Princeton : Princeton University Press, 2015.

Stavridis, James. 2019. Opinion: Poland Isn't Getting Its 'Fort Trump' – Yet. *Bloomberg News Wire.* [Online] BNN Bloomberg News Wire, June 13, 2019. [Cited: April 02, 2023.] https://www.bnnbloomberg.ca/poland-isn-t-getting-its-fort-trump-yet-1.1272992.

Uudeberg, Tiina. 2022. The exponential growth in the wartime composition of the Defence Forces was caused by the lessons of Ukraine. *ERR News (Estonian Public Broadcasting).* [Online] ERR (Estonian Public Broadcasting), July 6, 2022. [Cited: April 5, 2023.] https://www.err.ee/1608650302/kaitsevae-sojaaja-koosseisu-huppelise-kasvu-tingisid-ukraina-oppetunnid.

Veebel, Viljar and Ploom, Illimar. 2019. Are the Baltic States and NATO on the right path in deterring Russia in the Baltic? . *Defense & Security Analysis.* 2019, Vol. 34, 4.

—. 2018. Estonia's comprehensive approach to national defence: origins and dilemmas. *Journal on Baltic Security.* 2018, Vol. 4, 2.

Veebel, Viljar. 2021. Russia and Western concepts of deterrence, normative power and sanctions. *Comparative Strategy.* 2021, Vol. 40, 3.

Vseviov, Jonatan. 2021. *Constructing Deterrence in the Baltic States.* Tallinn : International Centre for Defence and Security, 2021.

MAJ (GS) Pascal RIEMER, PhD. Auftragstaktik and its implication on the military strategic level

Introduction

Auftragstaktik, the German military leadership concept that is probably best known beyond linguistic and cultural borders, has not least experienced its mystification due to the outstanding successes of the Prussian and German armies in the 18th to 20th centuries – Emperor Frederick the Great, Field Marshal Helmuth von Moltke the Elder or Colonel General Heinz Guderian to name a few protagonists here - when numerically inferior armed forces were always able to claim the battlefield victoriously for themselves (Muth, 2011 pp. 22, 173-174) (Shamir, 2011 pp. 29-53). Many armed forces have tried to adopt this supposed recipe for success as a leadership principle and implement it in their organisation.

However, as difficult as it is to find already an appropriate translation for this term in English, be it ‘directive control’, ‘mission-type-orders’ or ‘mission command’, the more difficult and complex it is to cognitively understand the concept, to ensure the appropriate framework conditions within the military culture and to implement *Auftragstaktik* in reality in the face of rapidly advancing technological change. Finally, this field of tension has led to a real debate, especially in the US military sciences, about the sense and nonsense of this leadership concept.

On the one hand, the supporters are convinced that *Auftragstakitk* as a cross-level leadership principle continues to be the most promising approach to solving complex military problems in the 21st century. They follow the core argument that regardless of technological progress and the specific level of war, the victor will continue to be the one who can not only make sound decisions in time but also execute these decisions faster and better than the adversary. *Auftragstaktik* as a decentralised approach would thus create better conditions to operate in the adversary's decision-making process, which the US military pilot and strategist John Boyd called the OODA Loop (Observe - Orient - Decide - Act) (Vandergriff, 2019 pp. 5-17) (Mattis, 2008 pp. 107-108).

On the other hand, opponents of *Auftragstaktik* see in this leadership model only an unpredictable disruptive factor in an increasingly digitalised world. The most prudent

way to penetrate the fog of war with its resulting variables of friction, probability, and opportunity according to Carl von Clausewitz would be the acceleration as well as expansion of accumulation and processing of information. Based on a near-perfect operational picture of the situation the deployment of down to the very last detail synchronised forces will guarantee military victory. By applying new technological achievements, such as artificial intelligence, the networking of sensors, systems, platforms, and effectors as well as the cross-domain transmission of data without any time delay, the fog of war could thus be lifted, making the prevailing chaos controllable (Owens, et al., 2001 pp. 12-15) (Lythgoe, 2020 pp. 35-36) (Hill, et al., 2017 pp. 99-100).

Although much research related to *Auftragstaktik*, whether agreeing or disapproving, focuses essentially on the tactical level, very little to no attention is paid to its relationship and interdependencies at the military strategic level of war. Given this research gap, the present article aims to shed light on the benefit or harm of *Auftragstaktik* at the military strategic level, especially concentrating on leadership and the outcome for professional military education (PME). To this end, this analysis will be focusing on two parts. Firstly, explaining *Auftragstaktik* from the perspectives of its historical roots, prerequisites, and functionality of the concept. Secondly, assessing the military strategic level by exploring the future military strategic environment, defining the development and implementation of a military strategy, as well as determining the characteristics of leadership at this level. Historical examples will be used, where they are deemed necessary to better contextualise the problem set. The analysis is based on a qualitative literature analysis of historical and doctrinal literature, memoirs, and classics of *Auftragstaktik* and strategy using the categories of Clausewitz's axis of purpose-aims-means as well as the factors of time-space-force that transcend all levels of war. Based on the findings, the conclusion answers the research question defined earlier, namely that *Auftragstaktik* is not only relevant but paramount for military strategic leaders to seize and maintain the initiative in future conflicts.

Understanding *Auftragstaktik*

Historical roots and prerequisites of *Auftragstaktik*

Historically, the starting point for the development of this concept, as exemplified by the Prussian and German armies, was always the political will to wage a war despite

military inferiority in terms of resources with the party to the conflict and of course, to win it. However, according to the military authorities of the time, this demanded a commitment to actively led, offensive operations, which in the best case would lead to victory in the initial phase of a war in order to prevent a long, resource-consuming war of attrition (Shamir, 2011 pp. 36-53) (Creveld, 1982 pp. 4-6). The concept of *Auftragstaktik* is therefore primarily aimed at undermining the enemy in terms of time and striking at an identified weak point with a spatially limited, force-based superiority (Boyd, 2007 pp. 79, 87). The latter is generally understood under the term *Schwerpunkt* [main effort], and is best expressed in particular by Heinz Guderian's famous quote: ‘Boot 'em, don't spatter 'em!’ (Guderian, 1960 p. 95) (Bevin, 1993 p. 227). This ultimately serves to achieve a moral or cognitive surprise effect on the opponent, which in the best case leads to a state of paralysis, i.e. the actual inability to act, whereby the opponent's will to continue the fight is defeated (Boyd, 2007 p. 87).

Since this leadership principle therefore dates back to a time when there was no question of communication without time delays, in contrast to the digital data transmission of the recent past or the present, the time advantage had to be achieved through a human-centric approach to increasing the quality of individual and organisational leadership performance. This primarily involved the cognitive domain of thinking and military cultural manners that applied to the individual decision-maker and groups alike. This framework included, among other things, critical, reflective, thinking, the need to deal with uncertainty and the unexpected, as well as the exploitation of opportunities that arise through self-initiative, which in turn motivates both the military leader and the subordinate. For the organisation, this means creating an environment that favours these individual conditions first and foremost. On the one hand, this is achieved through a pronounced ‘culture of error’, in which a person entrusted with a mission does not need to fear exorbitant negative consequences for a failure (Shamir, 2011 pp. 26-27) (Wittmann, 2012 p. 40) (Avidor, 2021 pp. XII-XIV). This is expressed in particular by the following quote from Frederick the Great: ‘It is pardonable to be defeated, but never to be surprised’ (Frederick the Great). However, this failure must be due to the self-initiative to fulfil the mission and, conversely, does not mean that the military leader is legitimised to become a free-floating radical who acts detached from all framework conditions.

Accordingly, as a further basic prerequisite of the organisation, the decision-maker must be granted a high degree of trust to fulfil the mandate given. This decentralised approach, which strengthens the position of subordinates at all levels through confidence, therefore places less emphasis on pronounced measures of control to verify the implementation of the commanded tasks (Shamir, 2011 p. 26) (Austrian MoD, 2004 pp. 39-40). This is because the organisation has the fundamental expectation that the independent fulfilment of the assignment will be successfully implemented even under very difficult and changed framework conditions.

To implement *Auftragstaktik*, the organisation must coordinate the training, education and upbringing, for the military decision-makers, in order to create a quasi-like-minded body of individuals in the area of problem-solving competence (Boyd, 2007 p. 74) (Austrian MoD, 2004 p. 40). Back to the specific requirements of *Auftragstaktik*, great emphasis is therefore placed on general education with a focus on the ability to network and understand interrelationships, rather than a pronounced specialisation in one subject area, primarily pursuing principle-led teaching to enable individuals to become lifelong learners (Muth, 2011 pp. 175-178). As a final organisational prerequisite, again using the example of the Prussian and German armed forces, a general staff corps was established within the framework of military elite formation, after demanding selection and further in-depth training. This corps, whose personnel share in the structure of the organisation increases with the ascending level of command, has the role of supporting the commander in his decision-making, planning and execution due to its highly developed cognitive abilities. In doing so, these general staff officers perform a hinge function in which they play a decisive role in the translation of the problem to be solved (Shamir, 2011 pp. 39-41, 121-122).

The concept of *Auftragstaktik*

The actual mode of operation of the leadership concept of *Auftragstaktik* at the tactical level can best be understood by first outlining the cornerstones of military problem solving, namely the purpose of the superior, the purpose of the subordinate, i.e. own, level, the objective to the subordinate level, the way to achieve the objective and finally the means provided by the superior level (Austrian MoD, 2013 pp. 87-91).

In the case of *Befehlstaktik* [order-type-tactics], the actual opposite of *Auftragstaktik*, a concrete specification is made by the superior command to the subordinate level in all

of the above-mentioned areas (see the left-hand illustration in Figure 1). These specifications are therefore immutable constants.

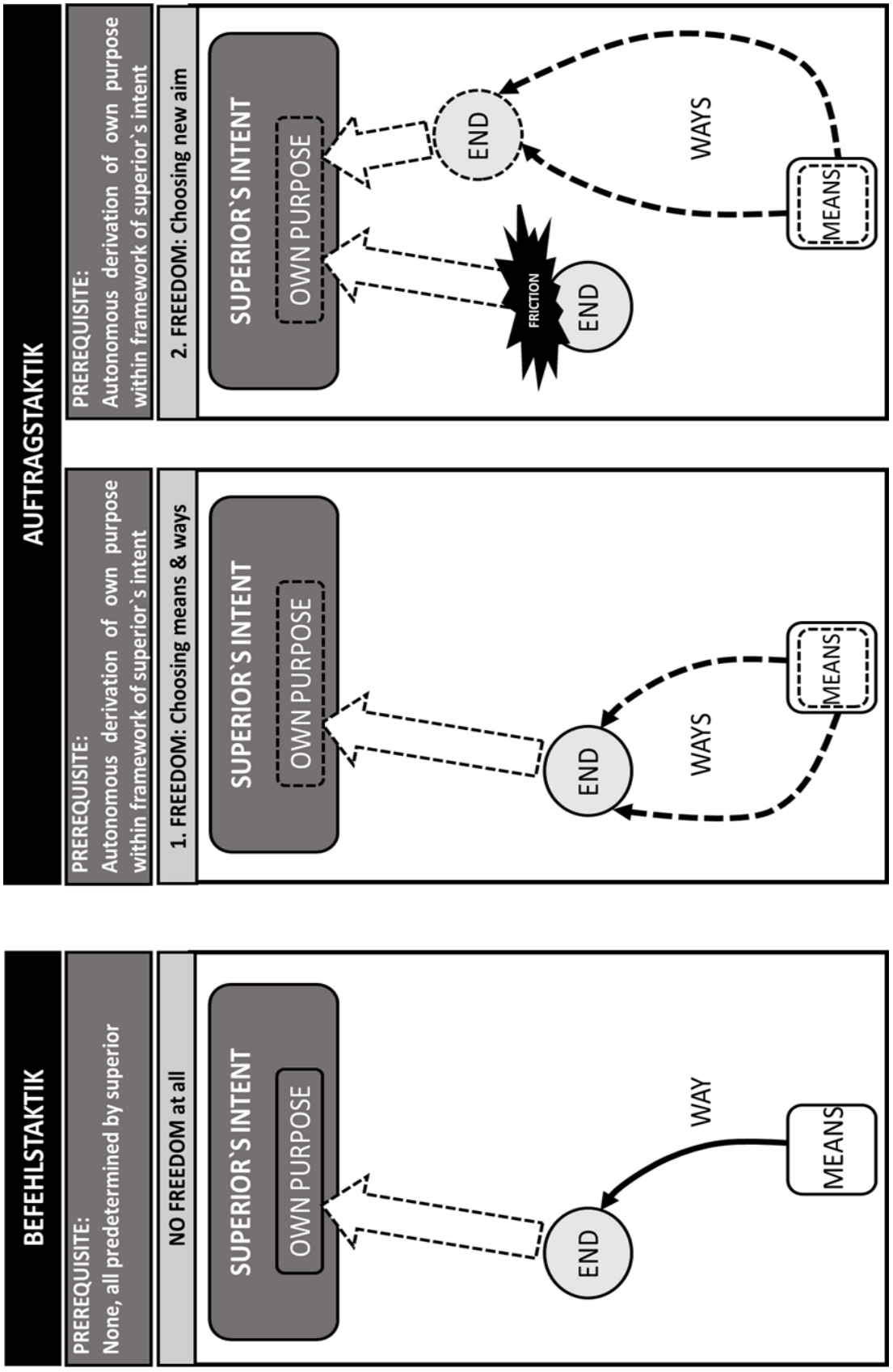


Figure 1: The mode of operation of *Befehlstaktik* and *Auftragstaktik*. Source: Author`s own.

The concept of *Auftragstaktik* deviates from these rigid specifications and leaves the independent assessment of these cornerstones of problem-solving to the subordinate level under certain framework conditions. In other words, in the concept of *Auftragstaktik*, some immutable constants become changeable variables. In this respect, two cases can be distinguished: The standard case and the case of the freely assessed intent, which is based on the overall framework of the regular case but deviates from the given mission. Regardless of this, in all cases the purpose of the higher command as well as the means made available are to be understood as constants that take on the function of a fixed bracket.

In the standard case the objective, which is received as a mission, takes on the function of a further constant. In connection with the purpose of the superior level this is necessary to independently comprehend one's purpose as the essential performance within the idea of the superior's battle order through brief reflection with the environment and the opponents. Based on this, the subordinate level is free to use the means provided at its own discretion, as long as no concrete additional restrictions have been given otherwise, in order to fulfil the mission and to contribute to achieving the purpose of the higher command (see the middle illustration of Figure 1) (Wittmann, 2012 S. 40) (Austrian MoD, 2004 pp. 39-40) (Austrian MoD, 2013 pp. 87-91).

If the situation changes so rapidly that there is no longer any connection to the superior and the achievement of the mission not only no longer makes sense, but also the fulfilment of the purpose of the higher command is endangered and immediate action is paramount, the case of the freely assessed intent occurs (Oetting, 2000 p. 353) (Austrian MoD, 2004 p. 39). This means that, derived from the essential performance and considering the new framework conditions, the received mission must be deviated from and a separate, self-derived aim may be determined as a new variable itself (see the right-hand illustration of Figure 1).

The method used here to make faster decisions and to translate them into faster actions than the opponent requires the leadership to be able to quickly reduce the complexity of a problem and to possess a high degree of creative potential and mental flexibility. In this context, *Auftragstaktik* is based on a decentralised leadership structure, which is characterised by the fact that communication between the

leadership levels takes place exclusively, both top-down and bottom-up, implicitly through the constant analysis and synthesis of the so-called Clausewitz axis, i.e. the correlation between purpose-aims-means, with a high willingness to take risks (Boyd, 2007 p. 79) (Vandergriff, 2019 pp. 12-17). John Boyd has described this characteristic in the following words:

> The secret of the German command and control system lies in what's unstated or not communicated to one another—to exploit lower-level initiative yet realize higher-level intent, thereby diminish friction and reduce time, hence gain both quickness and security (Boyd, 2007 p. 79).

Summary

In summary, it can be said that *Auftragstaktik* attempts to compensate for the quantitative lack of resources by increasing the quality of command performance. The actual hypothesis on which the concept is based is therefore: Deciding and acting faster, more effectively as well as efficiently than the opponent means prevailing on the battlefield. To achieve this, however, mistakes are consciously accepted with a high willingness to take risks and sacrifices are made in the explicit control of one's own forces based on an excess of trust. A Tayloristic, i.e. mainly process-oriented, top-down approach, which focuses on centrally controlled synchronisation and control with the greatest possible reduction of errors, is therefore diametrically opposed to successful *Auftragstaktik*. In the latter, the emphasis is placed on the assumption of decentralised self-synchronisation of the elements based on favourable opportunities arising in the field in conjunction with the military leaders' own initiative. An elite general staff corps is to ensure that the advantages of *Auftragstaktik* at the lowest tactical level are also transferred to higher levels of command. At the same time, this body of personnel should centrally ensure that the speed of decision-making at these levels is preserved by relying on the cognitive capacity to reduce complexity and the creative power for out-of-the-box options for action. The application of Auftragstaktik is thus primarily a result-oriented concept, whereby the preparation of personnel requires an emphasis on teaching of methods, principles, and broad knowledge.

The Military Strategic Level

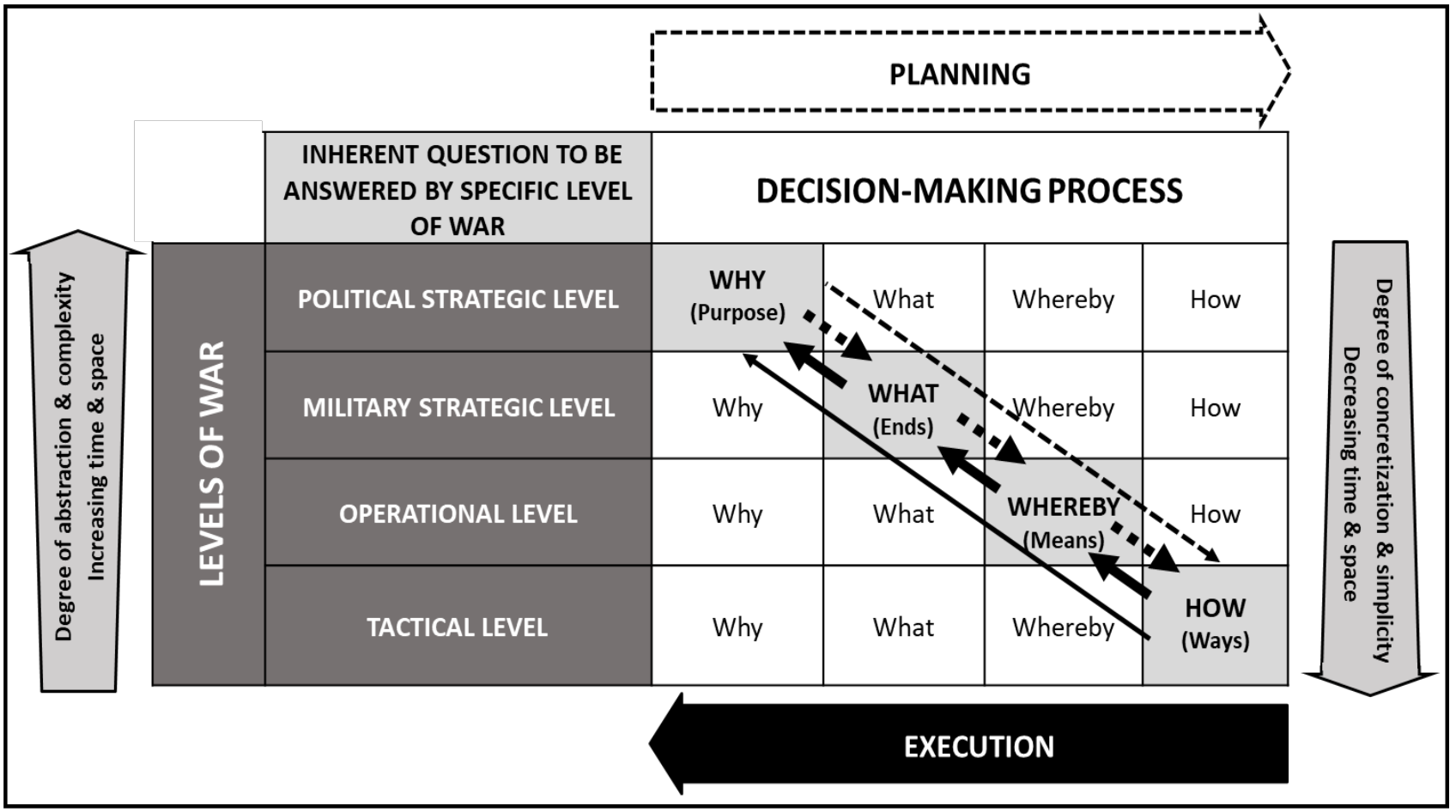
The future military strategic environment

One of the main arguments put forward by opponents of *Auftragstaktik* is that in future wars, the friction arising from the fog of war can not only be reduced but even

eliminated using technological developments. In this light, it makes sense to take a closer look at the corresponding future environment at the strategic level. Generally speaking, mankind is in a phase of transition, in which the industrial age has been replaced by the information age in connection with digitalisation. On the one hand, this is characterised by the fact that information of all kinds can be collected, processed, and distributed globally at a speed without time delay, whereby this happens both fully autonomous and semi-autonomous. On the other hand, artificial intelligence is able to link the information generated from this cycle on the basis of rational logic and to work out solutions. While the former merely represents a continuation of previous technological trends, this development leads to the fact that previous sharp demarcations of leadership levels, i.e. between the tactical, operational, military strategic and political strategic levels, threaten to become blurred according to the factors of time and space. A delimitation in time horizons or clearly defined areas of responsibility still seems possible, but with enhancing digitalisation, the probability of skipping one or more levels also increases, both in the top-down and bottom-up approach (Simonetti, et al., 2020 pp. 136-141).

If this makes the connection between the levels of war vertically permeable or dissolved, then artificial intelligence is already or will soon be able to do the same in a horizontal perspective. This means that the decision-making process of the OODA Loop described by Boyd, which essentially answers the big questions ‘Why?’, ‘What?’, ‘Whereby?’ and ‘How?’, meaning purpose, goals, means and ways, can be significantly shortened through artificial intelligence (see Figure 2). In its sharpest form, which already comes close to science fiction, the combination of both approaches would be hyper-centralised leadership. In other words, following the example of historical ‘strategic commanders’, such as Alexander the Great, the political strategic level could once again directly command the tactical level (Creveld, 2011 pp. 15-17) (Freedman, 2022 p. 500). However, the commanders of the phalanx would also become superfluous, whereby artificial intelligence would join the ranks of the atomic bomb in the Revolution in Military Affairs.

INTERACTION AND INTERDEPENDENCIES OF LEVELS OF WAR



Remark:

Possibility of both-sided skipping of levels in conjunction with inflictions in space-time-force

Figure 2 The interaction and interdependencies of levels of war. Source: Author`s own.

Even if the futuristic prospects presented here harbour a certain charm as well as technological promises of salvation, two further aspects must be taken into account in this context. The strategic environment of the future with an increasing flood of data will remain contested and unpredictable, as Europe had to learn at the latest with the Russian invasion of Ukraine starting on 24 February 2022 (NATO, 2022 p. 1). The common known expression for this unpredictability is summarised under the acronym VUCA, meaning volatile, uncertain, complex and ambiguous and is best described in the so-called Cynefin framework (MCDC, December 2020 pp. 13-15). The Welsh term Cynefin is understood to mean that multiple factors influence our environment in ways that people are unable to ever understand. In this respect, the Cynefin framework divides the challenges that arise according to the nature of the relationship between cause and effect, distinguishing between: simple, complicated, complex, chaotic (MCDC, December 2020 p. 14). In the era of the information age, it is assumed that the most difficult manifestation with so-called ‘whicked problems’, namely chaotic, will represent the norm. Here, it is usually not possible to establish a relationship between cause and effect at the system level (MCDC, December 2020 pp. 13-15). The suggested way for problem-solving is to do in such a chaotic environment the following: ‘[...] a leader must first act to establish order, sense where stability is present and from where it is absent’ (MCDC, December 2020 p. 15). The gap between human understanding and its environment, also called uncertainty, will thus continue to persist (Avidor, 2021 p. 296) (Freedman, 2017 pp. 279-280).

Another aspect to be considered in connection with the last quote is the nature of war as a human socio-political phenomenon. Even if the advancing technological achievements have changed the face in the form of the character of war over the centuries, its core always remains the same. Political interests are enforced through the military as a means of power utilizing demonstration, projection, threat or actual use of force (Clausewitz, 2008 S. 50). Starting from the decision-making to the unfolding of the effect, be it (un-) conscious, (in-) direct, (non-) lethal or (non-) kinetic, the focus of warfare is to exert an influence on the human will. This includes friendlies, enemies, or uninvolved persons. From this perspective, hyper-centralised command and control steered by artificial intelligence is unlikely to be realised in Western armed

forces in the foreseeable future, also due to the ethical concerns that cannot be dismissed out of hand. Regardless of this, it can be assumed that artificial intelligence will be assigned certain tasks at various command levels that can be implemented more quickly and accurately by a machine. In this context, however, humans remain the controlling, reviewing, evaluating and deciding body in these processes (Simonetti, et al., 2020 pp. 142-143).

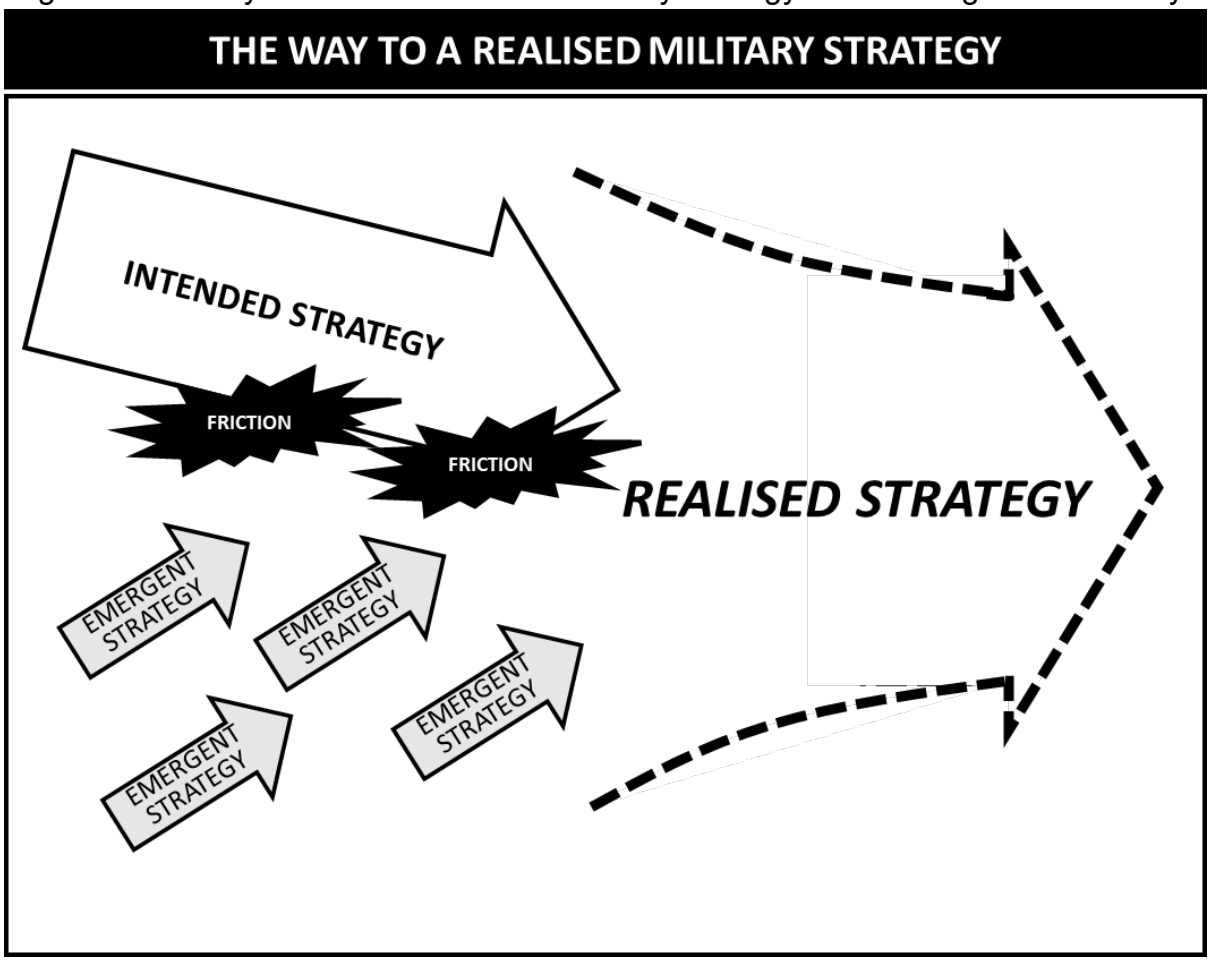
The development and implementation of a military strategy

Building on the compiled understanding of *Auftragstaktik* and the strategic environment, the essence of the military strategic level and military strategy itself must now be examined more closely in the areas of objective, planning and execution. Referring back to the term used by Carl von Clausewitz, military strategy turns out to be the use of battles for the purpose of war, whereby the individual engagements are combined into campaigns, and these in turn into a war plan (Clausewitz, 2008 S. 176-178). In other words, military strategy transforms and combines the expressed political will (focusing on ‘Why?’) with military action by formulating appropriate goals for this and providing the necessary means (focusing on ‘What?’) (Souchon, 2020 p. 17). This intentional, linear approach leads to the assumption that military strategy merely represents a deterministic sequence of a chain of causality and thus offers the appearance of immovable plannability. In this context, this plannability is also attempted to be transferred to the other, lower levels by shortening, limiting and concretising the areas of application in terms of time, space and forces (see Figure 2) (Jermy, 2011 pp. 210-215). Going further this means, that the operational level is the essential link that connects and synchronises the activities of the tactical level with the strategic goals and allocates resources to them (focusing on ‘Whereby?’). Whereas, the tactical level, on the other hand, is responsible for implementing the desired goals through military actions, or in Carl von Clausewitz's choice of words, engagements (focusing on ‘How?’) (see Figure 2) (NATO, 2023 pp. 58-59).

Such a perspective obviously favours a Taylorist hyper-centralised style of management, which, however, ignores an essential aspect in the implementation of strategies. This is the friction that arises in reality, creating uncertainty, which has already been aptly described in the above text as well as by Helmuth von Moltke the Elder: ‘No plan of operations extends with certainty beyond the first encounter with the enemy's main strength’ (Moltke, 1900 p. 291). Meaning in easier terms, that no plan

surpasses the first contact with the enemy. As a consequence, it can be deduced that military actions at the lowest level of command can have (un-) intended effects directly on a top-down, linear, intended military strategy. Or as the strategy researcher Colin Gray put it more concretely: ‘All military (tactical) behaviour has strategic weight, be it ever so small or even of net negative value’ (Gray, 2009 p. 8). The appropriate response must therefore be to adapt the military strategy to these frictions in the course of the execution of a military operation, to be able, despite everything, to turn the original idea into reality in order to achieve the given political purpose. Such an adaptation, to refer to the strategy model developed by Henry Mintzberg, can be called an emergent military strategy, whereby the synthesis of both strategies finally leads to the actually realised military strategy (see Figure 3) (Mintzberg, 2016).

Figure 3 The way to the realisation of a military strategy. Source: Figure created by



the author on the basis of Henry Mintzberg`s figure (Mintzberg, 2016)

The implementation of this theoretical view can be adequately illustrated by the example of processes implemented by NATO´s military strategic command, Supreme Headquarters Allied Powers in Europe (SHAPE). In this context, the Standing Defence

Plan (SDP), Contingency Plan (CONPLAN) and Generic CONPLAN represent the intended military strategies within the framework of Advance Planning, whereas emergent military strategies are described within the framework of Crisis Response Planning as so-called Operation Plans (OPLAN) (SHAPE, 2013 pp. 1-3). The latter are triggered by frictions that endanger the success of the former and are pointed out to the leadership by means of indicators and warnings (SHAPE, 2013 pp. 2-3 to 2-5).

In order to ensure the successful implementation of a realised military strategy, it is therefore indispensable to make use of two instruments that permanently and without interruption prepare the basis for decision-making for the leadership. On the one hand, this is an organisational entity for determining a current situational picture as a basis for the necessary target-performance comparison, in order to recognise a deviation of reality from the intended military strategy and, if necessary, to be able to counteract it with an emergent military strategy (Zinni, 2020 S. 114-115). Such events of particular importance can, in their most intensive manifestation, lead to the fact that deployed military strategic commanders must be informed at all times, so that they can make decisions without delay. US General (ret.) James N. Mattis ironically referred to this category of alerts as ‘night orders’ during his time as commander of the US Central Command (Mattis, et al., 2019 p. 199). On the other hand, however, an interface to day-to-day operations is also required at this level of command in order to be able to exert a controlling influence on the levels below (Zinni, 2020 S. 114-115). In the latter case, the possibility exists in this context to leapfrog several levels of command and even intervene directly in the action of a battle.

The characteristics of leadership at the military strategic level

After assessing the strategic environment as well as the general nature of the military strategic level, the individual and organisational requirements for future successful military strategic leadership must be explained from two different perspectives. In this context, however, one must always be aware that this primarily serves to enable successful combat at the tactical level, because only here effects can be achieved in all different domains.

Firstly, the innovation factor is emphasised by both former high-ranking military commanders and leading scientists. Since this primarily concerns material and technological advances, it is always necessary to strike a balance between wishful

thinking and real feasibility. What is essential, however, is not the technology itself, but the recognition of the associated possibilities of its use, i.e. conception (Adamsky, 2027 pp. 135-138) (Zinni, 2020 S. 24-36). At this point, we may recall the battle tank and its different applications in the Second World War. While the Allies used it mainly as a combat support weapon for the infantry in the initial phase of the war, the German Wehrmacht, largely under the development of Heinz Guderian, conceived of it as the main carrier in the battle of the combined arms, for the re-empowerment of manoeuvre-centred warfare, also known as *Blitzfeldzüge* [Blitz campaigns] (Guderian, 2018 pp. 221-268) (Creveld, 2011 p. 223). The military strategic leadership must therefore have the ability to anticipate and create the conditions for the implementation of a creatively thinking and learning organisation in order to remain adaptable in times of non-decreasing technological developments.

Secondly, this adaptability must also be transferred to the decision-making process to increase the speed of implementation of tactical actions and thus gain the initiative. Ultimately, this should be done by creating ‘battlefield harmony’, which is the opposite of one's own paralysis, and lead to the will of the opponent being defeated (Mattis, et al., 2019 p. 239). To achieve this, however, it would be necessary to review the organisational and processual structure according to its actual added value, depending on the respective individual situation, i.e. the quantitatively and qualitatively available personnel and material at all commanded levels. Or as General James N. Mattis put it: ‘We sometimes find that we`ve grown organisations with echelons that have outlived their value’ (Mattis, et al., 2019 p. 242). This adjustment affects both the vertical and the horizontal interaction and interdependencies of the levels of war (see Figure 2). Conversely, however, this means for the military strategic commander to have comprehensive, generalised knowledge of the capabilities and processes at hand in order to effectively steer the campaign. In the area of implementation, how these adjustments are to be made, namely either through centralisation or decentralisation, we come full circle back to the presentation made in the introduction between the proponents and opponents of *Auftragstaktik*.

Summary

In conclusion, the comprehensive assessment of the military strategic level has shown that, on the one hand, despite disruptive technological developments such as artificial intelligence, the uncertainty triggering friction will continue to exist and, on the other

hand, humans and their will continue to be at the centre of warfare. The friction leads in further consequence to the necessity of implementing emergent strategies in order to be able to translate an intended strategy into reality. Military strategic leaders must therefore possess certain traits with the purpose of gaining the initiative in a military confrontation over the adversary, undermining him in his OODA Loop in time and ultimately defeating him. This includes having a broad, general understanding of processes and military capabilities of all subordinate levels as well as being able to generate emergent strategies under time pressure. Furthermore, the military strategic leader must be able to recognise the real value of innovation, namely the benefits and opportunities of technological progress for the tactical level, and in this context promote the implementation of a creative thinking and learning organisation. Finally, the military strategic leader should have the ability and the courage to assess the organisational and processual structure in his area of responsibility according to its added value and, if necessary, to change it in order to accelerate the achievement of effects at the tactical level. Among other things, this also means skipping levels of war. In summary, it can be deduced that the essential characteristics relevant for planning and leadership at the military strategic level are the ability to anticipate, to recognise early and to adapt.

Conclusion

Before going into the synthesis in more detail, the most essential, derived core aspects of the topics dealt with are recalled once again. *Auftragstaktik* understood as a leadership philosophy, confers on subordinate commanders at the tactical level a relative freedom of action within the limits of the intent and purpose to be achieved by the higher level. This flexibility, coupled with decentralised self-synchronisation and a high willingness to take risks, is intended to enable decisions and actions to be taken more quickly than the adversary when frictions arise. This definitively results-oriented approach requires leaders to possess adequate cognitive capacity to reduce complexity as well as creative power, and the creation of a general staff corps attempts to transfer these advantages to other leadership levels. The training focuses on teaching methods, principles, and broad general knowledge.

As essential for planning and leadership at the military strategic level, it could be deduced that the qualities most needed are anticipation, early detection and adaptability in order to gain the initiative against an opponent and to be able to operate

in his OODA Loop. Accordingly, on the one hand, it is necessary to anticipate the benefits of disruptive technologies and to promote a creatively thinking and learning organisation. On the other hand, it is also necessary to create emergent strategies under time pressure in order to actually realise an intended strategy. For this, the existing organisation with its processes must be reviewed and, if necessary, modified, which requires a general in-depth understanding of these interrelationships.

The synthesis from these derivations shows that the requirements and results of both subjects of investigation are congruent to varying degrees of resolution. Both *Auftragstaktik* and contemporary as well as future leadership at the military strategic level seek to gain an advantage over opponents in an environment that is equally defined as uncertain, primarily through initiative. This is expressed first and foremost through the factor of time, namely based on mental flexibility to take and implement high-quality decisions in a timely manner. This attribute of being able to think and act both reactively and proactively in response to unforeseen events and new demands can also be summarised under another term, namely agility. This agility allows success to be generated even with fewer resources, especially when combined with identified adversary vulnerabilities and any deceptive measures to achieve surprise.

Even if technological progress accelerates the automation and autonomisation of warfare, the decision-maker ultimately remains the human being. Thus, combined with the continuing uncertainty, a decentralised approach to solving military problems at all levels of war offers the best conditions. Accordingly, it is the task of the PME in particular to create the foundations for such decentralised leadership. Firstly, the establishment of a military culture within the armed forces should be promoted that encourages risk-taking but also responsible action within legal and ethical norms and is characterised by an open culture of mistakes, or ‘honest mistakes’. Secondly, it would be appropriate for PME, at all levels of basic to general staff officer education, to primarily use a teaching method that emphasises the transmission of methods, principles and broad general knowledge and their implications for the military. In other words, the focus should be on imparting knowledge that will stand the test of time and consolidate it by applying it to contemporary problems. Consequently, the priority is not on transmitting overly specialised knowledge and rapidly outdated details. For contents may change, especially at the different levels of war, but the learned and internalised principles as well as knowledge about processes, and methods remain

essentially unchanged in their core. Accordingly, it can be summarised: Results-oriented decentralised leadership requires principle-led, process-oriented as well as broad knowledge-based education, training and raising.

Taking all these aspects into account, the following view of US Lieutenant General (ret.) Herbert B. McMaster can be explicitly agreed with:

> Leader development and education should promote an organizational culture in which higher-level commanders are comfortable with relinquishing control and authority to junior commanders while setting conditions for effective decentralized operations consistent with the doctrine of mission command (Shamir, 2011 pp. xii-xiii).

Bibliography

Adamsky, Dima. 2027. *The Culture of Military Innovation: The Impact of Cultural Factors on the Revolution in Military Affairs in Russia, the US, and Israel.* Stanford : Stanford University Press, 2027.

Austrian MoD. 2004. *DVBHzE Truppenführung [FM Unity of Command].* Wien : Austrian MoD, GZ S92011/42-GStbBür/2004, 2004.

—. 2013. *Lehrskriptum: Von der Taktik der Landstreitkräfte [Script: On Tactics of Land Forces].* Wien : Austrian MoD, Defence Academy, GZ S92012/4-LVAk/IHMF/2013, 2013.

Avidor, Gideon. 2021. Introduction. *Mission Command in the Israel Defense Forces.* Dahlonega : University of North Georgia Press, 2021, pp. VII-XV.

—. 2021. Mission Command and Non-linear Warfare. *Mission Command in the Israeli Defense Force.* Dahlonega : University of North Georgia Press, 2021, pp. 291-320.

Bevin, Alexander. 1993. *How Great Generals Win.* New York : W. W. Norton & Company, 1993.

Boyd, John. 2007. Patterns of Conflict. *Project White Horse.* [Online] January 2007. [Cited: 28 February 2023.] http://www.projectwhitehorse.com/pdfs/boyd/patterns%20of%20conflict.pdf.

Clausewitz, Carl von. 2008. *Vom Kriege [On War].* Hamburg : Nikol Verlagsgesellschaft mbH / Co. KG, 2008.

Creveld, Martin van. 1982. *Fighting Power. German and U.S. Army Performance, 1939-1945.* Westport : Greenwood Press, 1982.

—. 2011. The First and the Second World Wars. [book auth.] John Andrea Olsen and Gray S. Colin. *The Practice of Strategy. From Alexander the Great to the Present.* Oxford : Oxford University Press, 2011, pp. 219-235.

Frederick the Great. Inspiring Quotes. [Online] [Cited: 28 February 2023.] https://www.inspiringquotes.us/quotes/yDpk_YjeDcnP0.

Freedman, Lawrence. 2022. *Command. The Politics of Military Operations from Korea to Ukraine.* London : Allen Lane, Penguin Random House, 2022.

—. 2017. *The Future of War. A History.* London : Allen Lane, Penguin Randhom House, 2017.

Gray, Colin. 2009. *Schools for Strategy: Teaching Strategy for 21st Century Conflict.* Carlisle : US Army War College, 2009.

Guderian, Heinz. 2018. *Achtung – Panzer! Die Entwicklung der Panzerwaffe, ihre Kampftaktik und ihre operativen Möglichkeiten [Attention - Tank! Development of Tank Warfare].* [ed.] Sœnke Schenk. Nordhausen : Verlag Traugott Bautz, 2018.

—. 1960. *Erinnerungen eines Soldaten [Memories of a Soldier].* Heidelberg : Kurt Vorwinckel Verlag, 1960.

Hill, Andrew and Niemi, Heath. 2017. The Trouble with Mission Command. Flexive Command and the Future of Command and Control. *Joint Force Quarterly*, 2017, Vol. 86, 3rd Quarter, pp. 94-100.

Jermy, Steven. 2011. *Strategy for Action. Using Force wisely in the 21st century.* London : Knightstone Publishing Ltd, 2011.

Lythgoe, Trent J. 2020. Beyond Auftragstaktik: The Case Against Hyper-Decentralized Command. *Joint Force Quarterly*, 2020, Vol. 96, 1st Quarter, pp. 29-36.

Mattis, James N. and West, Francis J. 2019. *Call Sign Chaos. Learning to Lead.* New York : Penguin Random House LLC, 2019.

Mattis, James N. 2008. USJFCOM Commander's Guidance for Effects-based Operations. *The US Army War College Quarterly: Parameters*, 2008, Vol. 4th Quarter, 51, pp. 105-108.

MCDC. December 2020. MCDC Project: Future Leadership. [Online] December 2020. [Cited: 25 March 2023.] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/946243/20201210-MCDC_Future_Leadership-web.pdf.

Mintzberg, Henry. 2016. Need a Strategy? Let it Grow Like a Weed in the Garden. [Online] 13 October 2016. [Cited: 23 February 2023.] https://mintzberg.org/blog/growing-strategies.

Moltke, Helmuth, Graf von. 1900. *About Strategy. [Über Strategie].* Moltkes Militärische Werke. Berlin : Mittler & Sohn, 1900. Vol. 2.

Muth, Jörg. 2011. *Command Culture. Officer Education in th U.S. Army and the German Armed Forces, 1901/1940, and the Consequences for World War II.* Denton : University of North Texas Press, 2011.

NATO. 2023. *AJP-01 Allied Joint Doctrine.* s.l. : NATO, 2023.

—. 2022. *NATO Strategic Concept 2022.* Brussels, adopted by the Heads of State at the NATO Summit in Madrid, 29 June 2022 : NATO, 2022.

Oetting, Dirk W. 2000. Das Chaos beherrschen [Mastering the Chaos]. *Zeitschrift für Führung, Ausbildung und Erziehung*, 2000, Vols. Truppenpraxis, Wehrausbildung, 5, pp. 349-355.

Owens, William A. and Offley, Ed. 2001. *Lifting the Fog of War.* Baltimore : Johns Hopkins University Press, 2001.

Shamir, Eitan. 2011. *Transforming Command, The Pursuit of Mission Command in the U.S., British, and Israeli Armies.* Stanford : Stanford University Press, 2011.

SHAPE, NATO. 2013. *Allied Command Operations Comprehensive Operations Planing Directive V2.0.* Mons : NATO, 2013.

Simonetti, Rosario and Tripodi, Paolo. 2020. Automation and the Future of Command and Control. The End of Auftragstaktik? *Journal of Advanced Military Studies*, 2020, Vol. 11, No. 1, pp. 127-146.

Souchon, Lennart. 2020. *Strategy in the 21st Century. The Continuing Relevance of Carl von Clausewitz.* Cham : Springer Nature Switzerland, 2020.

Vandergriff, Donald E. 2019. *Adopting Mission Command, Developing Leaders for a Superior Command Culture.* Annapolis : Naval Institute Press, 2019.

Wittmann, Jochen. 2012. *Auftragstaktik - Just a Command Technique or the Core Pillar of Mastering the Military Operational Art?* Berlin : Carola Hartmann Miles-Verlag, 2012.

Zinni, Anthony C. 2020. *A Military Leadership and Organizational Innovation: A Case Study of the Pacific Theater in World War II.* Omaha : Anthony C. Zinni, 2020.

LTC Linas SADAUSKAS. Is Resistance an option for Lithuania?

Introduction

While addressing U.S. troops deployed in Lithuania President Gitanas Nauseda stated `the new reality and the threat posed by Russia force us to mobilize and place due emphasis on national defence and resilience´ (President of Lithuania, 2022). It might seem nothing new since 2014, though this announcement was made on 18th March 2022, in the aftermath of Russia's invasion of Ukraine, on the 24th of February (President of Lithuania, 2022; Steiner, 2022; United Nations, 2023).

This political announcement was made just one day after the Lithuanian Parliament (*Seimas*) passed the law on 17th March 2022, on the State Budget increasing defence spending of the year 2022 from a previously planned 2,2% to 2,5% of GDP (Seimas, 2022). Moreover, Seimas raised this sum to 2,52% for the year 2023 with a possibility of reaching 3% of GDP, if required (Seimas, 2022 p. 9). The Russian threat has been already considered since 2014 when Russia annexed Crimea and eastern Ukraine (NATO, 2014; NATO, 2015 pp. 3-4) and was firmly expressed in the National security strategy 2021 as an existential long-term priority threat for Lithuania (Seimas, 2021 p. 5). Yet, Russia's aggressive and unprovoked conventional invasion of Ukraine on February 2022 (NATO, 2022 p. 6) has shown both Lithuania and its Allies that Russian objectives are not limited to Ukraine, and it is aiming to re-write international rules and order, upon which global security stands (NATO, 2022 p. 6).

Already in 2014, to deal with the lack of conventional force to deter Russia, the U.S. Special Operations Command – Europe began a project with several allies, especially in the Baltic Region, to implement the Resistance Concept (Fiala, 2021 p. 3). The question now is, how should Lithuania implement national defence and resilience? Is resistance the best strategy for a small state defence?

This essay will argue that as a small state, Lithuania should rely on the main principles of the Resistance Concept in order to enhance the overall resilience of the state and to deter potential aggression from Russia. Nevertheless, due to the challenges associated with the provision of credible command and control, as well as, resourcing

the resistance, in a mid-term perspective, Lithuania should not envisage resistance as the main defence strategy for wartime.

To support this argument, this research paper will concentrate on the strategic application of the Resistance Concept to reinforce Lithuania's resilience and deterrence against Russia, focusing on the potential benefits of resistance. Then, the analysis will focus on two key aspects of organizing resistance, bearing in mind current internal and external geopolitical factors: facilitating reliable strategic command and resourcing resistance movement within occupied Lithuania. As the paper is based on open sources, it will not analyse or make conclusions and detailed recommendations of classified nature.

Exercising of the Resistance Concept – vaccination of the state and society?

To start with, the Concept of Resistance can reinforce the overall resilience of Lithuania and its deterrence against Russia.

Even though Russia is highly engaged with Ukraine and has faced heavy losses, it still has the potential to regenerate the offensive capacity to challenge the Baltic region (Paier, 2022 pp. 61-63; Mahda, 2022 pp. 83-85, 91; Ministry of Defence, 2023 pp. 4, 7-8, 18; Foreign intelligence service, 2023 p. 10). Consequently, despite NATO allies and nations themselves investing in the defence and prepositioning of forces, their efforts might not be adequate to credibly deter the potential aggression from Russia in the mid-term (Fiala, 2021 pp. 6-7; Shlapak, et al., 2016 pp. 1, 4). The quantitative calculations of RAND (Shlapak, et al., 2016 pp. 8, 12) with regard to force requirements to defend the Baltics might seem to be shredded by the qualitatively low performance of "the second army of the World", demonstrated in the Ukrainian front (Paier, 2022 pp. 61-62; Mahda, 2022 pp. 83-85). Yet, the perceptions and actions of the Russian government and society stipulate that strategic goals are not abandoned, and Russia is still keen to keep track (Ministry of Defence, 2023 pp. 4-5).

While a quantity may create a quality itself (Ministry of Defence, 2023 pp. 7-8), the supporting Resistance Concept can be the option to break a calculus of deterrence (Fiala, 2021; Fiala, 2022; Ministry of Defence, 2023; Fiala, et al., 2020; Stringer, et al., 2019 p. 2; Zdanavicius, et al., 2020). As a form of warfare, resistance is of non-

conventional and asymmetric nature. It introduces additional layers to a multi-domain battle space and projects a multiple set of dilemmas for a potential aggressor, to take into account. The calculation then might expand to its own force protection and significant forces to control an occupied area rather than just addressing conventional force (Fiala, 2021 p. 1; Stringer, et al., 2019 p. 16).

The Resistance Operating Concept, as well, emphasizes the importance of national resilience and defines it as the fundamental condition and critical cornerstone of national defence (Fiala, et al., 2020 pp. 25-26; Stringer, et al., 2019 pp. 5-7). As major general Kirk Smith (the former commander of Special Operations Command Europe) states in the Resistance Operating Concept, - 'Resilience is the fundamental foundation of Resistance' (Stringer, et al., 2019). Preparation for resistance, in turn, enhances an overall resilience of a state and sets conditions for total defence. It is a comprehensive approach in nature. Specifically, it considers the whole-of-government approach and encompasses the coordinated involvement of all state organizations. It is also defined as the whole-of-society approach as it involves the full spectrum of non-governmental entities, motivated by the defence of their motherland rather than the government or state institution. The involvement is based on the legal, therefore, credible framework (Fiala, 2022 pp. 15-16; Stringer, et al., 2019 p. 4) and drives both planning and preparation for crisis. The emphasis might range from the augmentation and training of personnel to the pre-stocking of equipment and supplies (Fiala, et al., 2020 p. 26).

The preparation requires an engagement of multiple institutions. As such, it might involve the Ministry of Justice (providing the legal framework for preparation and conduct of resistance), the Ministry of Transport and Communications (providing necessary contingency communications), the Ministry of Education Science and Sport (strengthening national identity, pride and cohesion), the Ministry of Finances and the Ministry of the Economy and Innovations (allocating necessary resources), Ministry of Defence (planning and coordinating the preparation for resistance and allocating personnel), etc. (Fiala, 2021 p. 15). Finally, it might involve the Ministry of Foreign Affairs and the Ministry of Defence gaining allied support (Fiala, et al., 2020 p. 25; Lithuania, 2023). Altogether, the focus is aimed to strengthen the awareness, confidence, and will of society to act and resist, thus enhancing its resilience to any

type of hostile foreign intrusion or crisis (Stringer, et al., 2019; Zdanavicius, et al., 2020).

To conclude, the numbers and facts of the ongoing attrition war in Ukraine are tempting the belief that the Russian army will not pose any significant threat in the Baltic region and there is an imminent end of the so-called “second greatest power in the World”. Russia’s regime, though, is still in power and it projects its strategic assertiveness reinforced by internal popular support for the war (Watling, 2023). It is still aiming to change the balance in the region. Though qualitatively failed, Russia preserves the potential to regenerate quantitatively and, therefore, to challenge both Euro-Atlantic and the Baltics. NATO allies and Baltic countries individually are taking resolute and intensive measures to change the balance in the Allies’ favour, though altogether that might not be enough in the mid-term.

Resistance might be the immediate conceptual and practical option to multiply the deterrence effect on Russia. Planning and preparation for resistance strengthen the resilience of society and the state. The expectation to encounter a resilient state prepared to total defence (including a phase of resistance), has a fair chance of expanding the calculations of Russia. As resistance expands a fight from conventional to non-conventional, it might create a complex set of dilemmas and multiply the number of dimensions (from whole-of-government to whole-of-society) to be faced. Therefore, this is in the Lithuanian government’s interest to introduce and coordinate comprehensive whole-of-government and whole-of-society mechanisms for planning and preparation of the state resistance as it strengthens state resilience and deterrence (Fiala, 2021). Yet, there are some dilemmas which need to be addressed and which will be tackled in the following two sections – establishment of a viable Command and Control (C2) system and resourcing of resistance.

Dilemmas of resistance. Command and Control in an occupied small state.

Legal and valid strategic command and systemic control of the resistance have still several key aspects to be addressed before becoming the leading concept for Lithuania’s defence.

To start with, the resistance C2 will certainly experience increased pressure from the Russian side (as it has been recently witnessed in Ukraine) in a considerably confined and contested space, as Lithuania's territory and demography is (Statistics Department, 2022; Petit, 2022 pp. 134-135). Outnumbered and technologically superior by the occupying force the Lithuanian resistance command might find itself exposed and compromised by occupying security services (Petit, 2022 p. 135).

As the enemy will try to detect, infiltrate and neutralize the resistance movement, the underground structure will face the dilemma of choosing between a centralized and decentralized way of command (Stringer, et al., 2019 pp. 38-40; Stringer, 2021 pp. 130-131). If the centralized approach was chosen, it could provide better control and cohesion of dispersed resistance entities. It could help to retain legitimacy and political unity of effort, as well. Yet, a hierarchic structure would naturally create weak spots due to its considerable predictability, consequently, could be much easier infiltrated and then destroyed (Stringer, 2021 p. 127). Therefore, this organizational design combined with the operational environment in Lithuania would require a level of security difficult or even impossible to exercise (Stringer, et al., 2019 pp. 24, 38; Stringer, 2021 p. 127).

The decentralized approach might present a resilient solution with regard to hostile penetration as it is difficult to track, systemize and overtake. It delegates a high level of authority and responsibility to the lower level of command and facilitates flexibility regarding dynamic conditions (Stringer, 2021 p. 127). Yet, considering the complexity of imposing an ethos of mission command, the operational dispersal factor and Russian counter-communication capabilities and experience, such a model could pose the risk of failing the control and, thus authority over the resistance, as well (Petit, 2022 pp. 134-135; Stringer, 2021 p. 127).

The aspect of communication will make C2 even harder to achieve both in the centralized and especially in the decentralized structure. If compromised, it will certainly result in the destruction of the resistance element or even the resistance as a whole (Stejskal, 2022 p. 39; Stringer, et al., 2019). The recent conflict in Ukraine is a straightforward example (exercised from both sides) of how electronic signals can be captured and identified as suspicious communications, with a help of Signal Intelligence capabilities. When the sender's location is pinpointed, targets are either

denied communication by electronic countermeasures or engaged mostly by indirect fires. This is especially evident towards radio and cellular signals. The application of alternative technologies and techniques (like using satellite internet, dispersing forces, introducing own electronic countermeasures, conducting signal deception and following communication security procedures) have been helping to overcome the latter threat (Petit, 2022; Stejskal, 2022; Zabrodskyi, et al., 2022).

Facing the historical experience of Russia's ability to deny shadow governments in occupied territories, the Lithuanian underground might choose to lead the resistance from exile. A positive aspect of leading and commanding the resistance movement from exile is that it might have direct representation and extension of the state sovereignty regarding Allies and partners. The government in exile may comparably unrestrictedly operate and communicate distanced from the occupier's control (Stejskal, 2022 p. 35; Stringer, 2021; Stringer, et al., 2019 p. 12). This method, however, will face two barriers to overcome.

First, as was described above, because of Russian technological superiority and experience to intercept communications, credible C2 will be considerably harder to achieve. By tracking and neutralizing underground communication networks Russia can eliminate or at least minimize communication to the less effective ways and means. Consequently, the government would find it challenging or even impossible to influence the processes in the occupied territory of the state. By tracking and infiltrating resistance communications Russia can interdict or deny C2 from inside. It can compromise the resistance movement and break it down (Petit, 2022; Stejskal, 2022; Stringer, 2021). Moreover, by infiltrating communication of resistance and monopolizing strategic messaging Russia can discredit the resistance movement both in the eyes of occupied society and of foreign Allies (Fiala, et al., 2020; Stringer, et al., 2019).

Despite the important advantages of the legitimate government in exile, it might face difficulty to sustain the legitimacy and confidence for an extended period in the eyes of locals, just because it is far away from all grievances and suppression the population is facing. Distant and safe decisions of the government could cause extended risk to the stay-behind society and even the resistance groups, thus breaking the cohesion of all-of-society resistance (Stejskal, 2022).

All in all, in the case of Russia, the Lithuanian underground resistance network will have to balance the clandestine-cellular command structure and the relevant level of control (Stringer, 2021). Though dispersed cellular fighting units will be more versatile and resilient under the punitive control of Russia, the decentralized structure will erode communications. Without centralized political-military guidance, resistance fighting might turn ineffective or even counterproductive, as isolated units might lose their discipline and start targeting wrong targets, including civilians (Abrahms, 2018 pp. 126-131). Therefore, bearing in mind successful underground movements, the centralized military-style C2 (from the regional level up to the strategic) have to be established prior to conflict and sustained through all phases of the resistance. This will help to avoid the bear traps of ad hoc centralized organization. A particular emphasis must be given to secure and viable means and methods of communication as they will determine the effectiveness and survivability of the movement. In broader terms, it will provide legitimacy and confidence in the resistance, as well (Abrahms, 2018 pp. 126-129; Petit, 2022; Stringer, 2021).

Dilemmas of resourcing resistance under Russian occupation.

Successful resistance in Lithuania might be hard to attain under the Russian occupation if measures are not taken to address key principles of resourcing the resistance.

As the final aim of state resistance is to regain the sovereignty and territorial integrity of the state, the freedom fight must be conducted long enough or intensively enough to reach the goal. It is critical, therefore, not only to efficiently organize and lead the resistance network. All those comprehensive networks and fighting forces might appear worthless if they are not resourced for an extended fight. First, they will require all basic daily needs to sustain their life (Maslow, 1970). Additionally, they will require critical equipment, supplies, maintenance and services (including medical) to sustain their resistance actions and to overcome an occupier in the long run. Or they will have to survive long enough till incoming Ally forces. Coordinated and more extensive actions to support the liberation will accordingly require additional preparations, gathering and pre-stocking of weapons, equipment, ammunition, explosives, food and medical supplies. This will be especially challenging and important with a clandestine

nature of resistance, due to severe control and denial, imposed by an occupier, as well (Stringer, et al., 2019 p. 55; Anderson, 2005).

Recent Russian actions in the occupied territories of Ukraine prove the complexity of sustaining both violent and non-violent resistance. Russians have imposed harsh surveillance and severe control of the entire occupied populace from the moment they seized the ground. They established a proxy government, suppressed any opposition, provided “automatic citizenship” and implemented martial law or at least were targeting any suspicious activities, first (Diamond, et al., 2022 pp. 22-29; Skrypnik, et al., 2016; VOA, 2022). This restricted any freedom of movement of civilians, including members of the underground (Stringer, et al., 2019). Aimed to intimidate and subdue the society to Russian rule and prevent the appearance of any pockets of resistance, occupiers have come to war crime measures. The destruction or control of vital infrastructure, unexpected searches and looting, identity checks and arrests of civilians, interrogation and killings, rape and sexual violence, mass murders and the state of humanitarian crisis have become daily life of the locals (Diamond, et al., 2022 pp. 22-34; Prosecutor General's Office, 2023 pp. 7-36, 58-59; Quinn, 2015; Shynkarenko, 2022; Skrypnik, et al., 2016 pp. 43-44; VOA, 2022; Yaffa, 2022). Anyone who is slightly suspected to be a member of Ukrainian armed forces and is of conscription age or suspected to have any relations to them has been seized or shot (Diamond, et al., 2022 pp. 22-25; European Commission, 2022; Kortava, 2022; MSN News, 2022; Prosecutor General's Office, 2023 p. 25; UNHR, 2022). In such circumstances, it is hard to imagine establishing a credible functioning supply system from the scratch. Only when the occupier and its proxies get grip on the ground and the situation relatively calms down (by switching to semi-denied mode), resistance might emerge (Stringer, et al., 2019).

For the resistance to emerge and succeed, the financial function must be emphasised, as resistance will require money. Though sustaining the underground organization heavily depends on auxiliary force, daily resourcing of additional “family members” for an extended period will become a hard burden to endure for the population which suffers the aftermath of conflict. Motivation depleted due to the long-lasting pressure might turn into indifference and even hostility, thus undermining the support. Therefore, the resistance will require funds to compensate for the demand. The demand for shelter, food, supplies, materiel and services. Money will be required to bribe officials of occupying governance for silence, information, accessibility and freedom of action,

fake identity and jobs, etc. Last, but not least, the shadow government will require to sustain its social system, typically for auxiliaries (Stringer, et al., 2019). Historic and the most recent examples of Russian actions in occupied territories prove financing of resistance extremely difficult. The very moment Russians get grip on a territory, they start an integration process. Apart from political integration (an introduction of “local” governance and “automatic citizenship”), they are proceeding with monetary integration, as well. This refers to the introduction of unitary currency and transactions in the Russian Rubble, making any official financial transactions controlled by occupying regime and any opposing markets pushed out or slipped underground (Charron, 2020; Orlyk, et al., 2022; Patrakeeva, 2015 p. 59).

To sum up, recent events in Ukraine have proved that Russian occupiers will do all that is in their power to deny any kind of opposition and to establish uncontested control over territories seized. They will not limit themselves to targeting combatants or even prisoners of war (who might potentially become the bulk of guerrilla force later), they will commonly use military power to target and intimidate civilians, who could constitute auxiliaries of the resistance. If opposed, without any hesitation Russians will destroy necessary infrastructure and will deprive civilians of resources. The sparse supplies will be limited in access or controlled by occupying force and available only with a Russian passport (Skrypnik, et al., 2016), thus sustaining the living of potential supporters at the level of basic needs and leaving no reserve to share with freedom fighters. To make matters worse, occupying regime will introduce its currency as soon as possible centralizing finances and controlling financial transactions. Therefore, if not pre-stocked, an ad hoc organizing of resources and services necessary for the underground organization will require an extended period following the conclusion of an active conventional fight. The latter applies to financial resources, as well. Moreover, it brings the dilemma of either investing in the shaky Russian Rubble or relying on the black-market “hard currency” (like Euro and Dollar) and Bitcoin. Even creating schemes to obtain money by relying on alternative and/or foreign sources cannot be excluded to overcome Russian control (Stringer, et al., 2019).

The comparison of the post-WWII and the contemporary resistance

The relevance of resistance (through the provision of resilience and deterrence, and considering the structuring, commanding and resourcing of resistance) should be also

assessed by comparing historical experience from the post-World War II (post-WWII) resistance and the resistance against Russian occupation, in the contemporary situation.

Exercising resistance in Lithuania has its historic heritage starting with 19th-century rebellions against the Czar regime (Encyclopaedia, 2022) and culminating with the freedom fights against the Soviets in 1940 and 1944 – 1965. The post-WWII resistance is recognized as the most well-organized and the most extensive one among the Baltics. As such, it was never planned and prepared prior to the occupation (Stringer, et al., 2019 pp. 159-160), therefore cannot be tested as a deterrent factor against an aggressor. Nevertheless, it demonstrated a high degree of resilience, and high involvement in society (with an estimated 4 % of active personnel among the population) and featured all classical elements of resistance organization with the shadow government, underground, auxiliary and military-style guerrilla force, capable of conducting active fight till 1953 (Stringer, et al., 2019 pp. 159-162, 168-169). With the absence of a legitimate Lithuanian government, it was the resilient society which formed the first resistance groups of the Lithuanian Activist Front already in 1940 (during the oppressive conditions of the first Soviet occupation) and the resistance organization (run by the Supreme Committee for the Liberation of Lithuania) in 1944, during the second Soviet occupation. The strong national identity, inherited from the independent state, constituted the basis of the resilience and, thus, for the prolonged resistance, as well. (Stringer, et al., 2019 pp. 160, 169).

As mentioned above, the resistance was structured and organized in a classical way, with the shadow government, supporters and fighters. The demography of that time (with an average of 69 % of the population living in rural areas) stipulated the proportionality of the resistance organization towards auxiliary and guerrilla-heavy, with more violent military actions. And only when this component was suppressed by 1953, the resistance shifted to non-violent actions only, organized by the few remaining underground activists in urban areas (Statistics Department, 1974; Stringer, et al., 2019). The clandestine structure of the post-WWII resistance was organized in the military style and decentralized at the lowest tactical level. This was determined by the experience from the initial fights of 1944-1946 when larger centralized units were easier located and destroyed by the superior occupying force. The communication was conducted through messengers and proxy mail. It was considerably safe, though

arguably too slow for mobile joint operations. As well, along with the model of decentralized organization, it made the exercising of legitimate control of units difficult to achieve. While no measures were taken from the Government side to prepare for the resistance prior to occupation, communication with the West was not planned and was non-existent from the very start. Any attempts to establish one failed. Therefore, coordination with outside allies or possible government-in-exile was absent. Consequently, there was no support from the outside, as well (Stringer, et al., 2019 pp. 161-165, 168-169).

As ‘resistance alone cannot free a country’ and ‘external intervention is necessary for liberation’ (Stringer, 2021 p. 129), the failure of gaining Ally support, must be emphasised separately. To start with, the main resistance strategy to liberate the state was based on active resistance with the assistance of Western allies (Stringer, et al., 2019 p. 163). This strategy both sustained the will to resist (resilience) and addressed the limited resources the resistance had to survive, fight and regain independence. Nevertheless, it was faulty from the very beginning as was grounded on false assumptions, deriving from the goals of the Atlantic Charter. With the lack of pre-war agreements, the West had no political obligation to support Lithuania and already agreed on the post-WWII World order at Yalta Conference. Finally, there was no legitimate government-in-exile or credible communication with the shadow government in occupied territory to convince them otherwise (Stringer, et al., 2019 pp. 159-169).

With foreign support missing, the “Forest brothers” had to sustain the resistance on their own. Initially, the post-WWII period favoured them with an abundance of German and Soviet weapons and ammunition left after the war. Nevertheless, due course they run out of supplies and could sustain just low-intensity activities (predominantly against collaborators and colonizers), only. Critical food supplies, shelter and other commodities were provided by the vast network of more than 80000 farms, whose food production rate might be compared to the contemporary level (Klupsas, 2022). Though the forestation level was 14 % lower than today (19 % of post-WWII compared to 33 % of current), it provided them relative freedom of movement and shelter, as well (Kairiukstis, 2021; State Forest Service, 2022; State Forest Service, 2022 p. 29). However, the Soviets finally effectively addressed auxiliaries by taking suspected farmers (and their families) to Siberia and centralizing (thus controlling) food production within collective farms. Along with increasing pressure from security services and

decreasing population support, this made the active resistance fade (Stringer, et al., 2019 pp. 166-167).

From the contemporary perspective, the historical experience of post-WW-II resistance demonstrates the importance of building national identity and resilience for an overall resistance of the state, even though, the resistance itself has not been planned. Considering the actions Russian aggressor normally undertakes in occupied territories (as was described in previous chapters), it would be wise to mimic the decentralized cell model at the tactical level, though sustaining centralized political-military control over all resistance organizations, to facilitate legitimacy and unity of effort. In this respect, the basic structure must be pre-established, legitimized and communicated among locals and Allies to gain recognition. Also, the C2 composition must be tailored to existing demographics. With 68 % of the current population being urban (Statistics Department, 2022), the C2 would balance towards underground and auxiliary heavy, with a minor guerrilla force and, therefore, fewer military actions. Larger military actions would not be advised, also bearing in mind the negative consequences of active fights of the “Forest brothers” and the Russian historical experience in suppressing active resistance.

Finally, the historical example of Lithuanian resistance after WWII demonstrates that liberation of an occupied state is not possible with a resistance movement alone. External support is vital both for the existence of resistance and for liberation, too (Prados, 2009 p. 28; Sheehan, 2015; Sliwa, 2022; Stringer, et al., 2019 pp. 129-141, 158-169). Moreover, resistance must be resourced in advance with shelter and basic supplies (of food, weapons, ammunition and medicine) to survive till the Allies come. Communications (both internal and external) are the key to capitalize effective and credible resistance, as well.

Conclusions and recommendations

The analysis of the possible contemporary application of the Resistance Operating Concept to enhance Lithuania’s resilience and deterrence against potential aggression from Russia has proved that both theoretical and practical considerations are still relevant. Universal principles of resilience and resistance could serve the state and society in the comprehensive preparation for total defence, or any kind of crisis

imposed by Russia or other states. The effectiveness of deterrence, though less easy to measure, still can be enhanced by expanding the quantity and quality of challenges the potential aggressor could face if decided to engage Lithuania. In this respect, the challenges posed to an adversary could expand from the military (state and Allies) dimension to the full spectrum of the civilian-military (whole-of-government, whole-of-society and Allies) dimension.

From a practical point of view, the preparation for resistance will require measures, normally taken to facilitate the prosperity of the state and to prepare for crisis management, including war. What is specific though, organizing the underground organization requires time and can be managed only when the security situation, imposed by an aggressor, allows it to do so. Bearing in mind lessons identified from the past and most recent conflicts (in which Russians have taken part), this could be hard to achieve even with external support to the underground organization. Therefore, it is recommended that the preparation for resistance should be taken by the Government before the crisis. It must be legally based and communicated to have legitimacy both in the eyes of Lithuania's population and the Allies. Communication is key to delivering the expected deterrent effect to a potential aggressor, as well.

If well prepared in advance, the resistance will have larger chances to survive and deliver the effects anticipated by the government and Allies. To do so, the organization of Lithuanian resistance must be structured in a balanced way to provide the clandestine C2 that sustains legitimacy and an alignment with the liberation goal. A decentralization of C2 might be considered at the lowest level only, to facilitate a relevant level of security and counterintelligence. Nevertheless, it still must be controlled by technical (pre-established and pre-supplied secure communication ways and means) and cognitive measures (as a practical application of the "mission command" philosophy).

Moreover, the contemporary resistance organization cannot be balanced in the way it was during the freedom fight of the "Forest Brothers" as the demographical situation has drastically changed since. If organized now, the resistance must be an underground-heavy, with both underground and auxiliaries concentrating in urban areas, with a relatively small fighter (guerrilla) force operating in a rural environment. The anticipated survival and effectiveness strategy might be based on historical

observations, final goals and the composition of the organization, itself. The movement must abstain from active kinetic actions as those will require a substantial level of preparation and resourcing (which will be extremely limited in an occupier-controlled terrain) and will certainly draw punitive actions from an occupier both towards the resistance and population, as well. Instead, pre-conflict and conflict clandestine preparation (including resourcing) should be considered for survival until and through the combined liberation along with the Allies. The Lithuanian NATO membership makes it feasible (NATO, 2022 p. 6).

To sum up, the analysis of the historical case study of post-WWII resistance in Lithuania and contemporary examples from Ukraine suggest that resistance alone cannot free occupied territories or state and external support is required. Therefore, despite the supporting relevance of the Resistance Concept to an overall preparation for total defence and deterrence, it cannot be considered the main defence strategy for Lithuania. It should be envisaged as one of the components and as a coordinated preparation for the defence and prudent building of state resilience, instead.

Bibliography

Abrahms, Max. 2018. *Rules for rebels. The science of victory in militant history.* Oxford : Oxford University Press, 2018.

Anderson, Rodney D. 2005. Lessons from history on the limits of imperialism: successful small state resistance to great power aggression. *Journal of Third World Studies.* 2005, Vol. 22, 1.

Charron, Austin. 2020. Russia's Recolonization of Crimea. *Current history.* 2020, Vol. 119, 819.

Diamond, Yonah, et al. 2022. *An Independent Legal Analysis of the Russian Federation's Breaches of the Genocide Convention in Ukraine and the Duty to Prevent.* Washington : New Lines Institute for Strategy and Policy, Raoul Wallenberg Centre for Human Rights, 2022. p. 47.

Encyclopaedia. 2022. Lietuva Rusijos imperijos valdymo metais (1795-1914) [Lithuania under the rule of Russian empire (1795-1914)]. *Visuotine lietuviu enciklopedija [Lithuanian Encylopaedia].* [Online] 2022. [Cited: 29 March 2023.] https://www.vle.lt/straipsnis/lietuva-rusijos-imperijos-valdymo-metais-1795-1914/.

European Commission. 2022. *Russian war crimes in Ukraine: EU supports the International Criminal Court investigation with €7.25 million.* Brussels : s.n., 2022.

Fiala, Otto C. and Petterson, Ulrica. 2020. ROC(K) Solid Preparedness: Resistance Operations Concept in the Shadow of Russia. *Prism : a Journal of the Center for Complex Operations.* 2020, Vol. 8, 4.

Fiala, Otto C. 2022. Legitimizing the Resistance. *Journal on Baltic Security.* 2022, Vol. 8, 1.

—. 2021. Resistance Resurgent: Resurrecting a Method of Irregular Warfare in Great Power Competition. *Special Operations Journal.* University of Maryland, 2021, Vol. 7, 2, p. 3.

Foreign intelligence service. 2023. *International security and Estonia 2023: Russian armed forces and the war in Ukraine.* s.l. : Estonian foreign intelligence service, 2023.

Kairiukstis, Leonardas. 2021. Lietuvos misku ukis [Lithuania's forests]. *Visuotine lietuviu enciklopedija [Lithuanian Encylopaedia].* [Online] 2021. [Cited: 29 March 2023.] https://www.vle.lt/straipsnis/lietuvos-misko-ukis/.

Klupsas, Feliksas. 2022. Lietuvos zemes ukis [Lithuania's agriculture]. *Visuotine lietuviu enciklopedija [Lithuanian Encylopaedia].* [Online] 2022. [Cited: 29 March 2023.] https://www.vle.lt/straipsnis/lietuvos-zemes-ukis/.

Kortava, David. 2022. In the Filtration Camps. *New Yorker.* 2022, Vol. 98, 32.

Lithuania. 2023. *My Goverment.* Vilnius : The Government of the Republic of Lithuania, 2023.

Mahda, Yehven. 2022. Putin's war in Ukraine. The background and anatomy of Russian aggression: The main war of the century: preliminary results. *Estonian Journal of Military Studies.* 2022, Vol. 1.

Maslow, Abraham H. 1970. *Motivation and personality.* New York : Harper and Row, 1970.

Ministry of Defence, Republic of Estonia. 2023. *Russia's War in Ukraine: Myths and Lessons.* 2023.

MSN News. 2022. *Russia-Ukraine war: Zelenskyy vows revenge as video of POW's 'murder' after last cigarette drag haunts world.* 2022.

NATO. 2022. *NATO 2022 Strategic Concept.* Brussels, Belgium : NATO Public Diplomacy Division, 29 June 2022.

—. 2014. NATO leaders take decisions to ensure robust Alliance. *North Atlantic Treaty Organization.* [Online] 5 September 2014. [Cited: 18 March 2023.] https://www.nato.int/cps/en/natohq/news_112460.htm?selectedLocale=en.

—. 2015. *Secretary General's Annual Report 2014.* Brussels, Belgium : NATO Public Diplomacy Division, 2015.

—. 2022. *The Secretary General's Annual Report 2021.* Brussels, Belgium : NATO, 31 March 2022.

Orlyk, Svitlana and Tsyganenko, Lilija. 2022. Financial and Economic Policy of The Russian Occupation Regime in Eastern Galicia and Northern Bukovina during the First

World War: Modern Scientific Discourse. *Journal of Danubian Studies and Research.* 2022, Vol. 12, 1.

Paier, Anton. 2022. Putin's war in Ukraine. The background and anatomy of Russian aggression: Russian capabilities in conventional high intensity warfate. Lessons from the 2022 invasion in Ukraine. [ed.] Vladimir Sazonov and Andres Saumets. *Estonian Journal of Military Studies.* 2022, Vol. 1.

Patrakeeva, Olga. 2015. О сценариях сотрудничества приграничных регионов России и Украины в условиях неопределенности [About scenarios of cooperation of border regions of Russia and Ukraine in the conditions of uncertainty]. *Regionalnaja Ekonomika. Iug Rossi.* 2015, Vol. 10, 4.

Petit, Brian S. 2022. Finding Order in Chaos: Conceptualizing Resistance Command and Control Approaches. *Journal on Baltic Security.* 2022, Vol. 8, 1.

Prados, John. 2009. Laos the road to Vietnam. *The Quarterly Journal of Military History.* 2009, Vol. 21, 4, p. 26.

President of Lithuania. 2022. The President met with U.S. troops at the Pabrade training area. *President of the Republic of Lithuania.* [Online] Office of the President of the Republic of Lithuania, 18 March 2022. [Cited: 30 January 2023.] https://www.lrp.lt/en/media-center/news/the-president-met-with-u.s.-troops-at-the-pabrade-training-area/38050.

Prosecutor General's Office. 2023. *On the frontline of Justice. Russia's War Crimes Factbook.* Kyiv : Government of Ukraine, 2023.

Quinn, John M. 2015. Notes from the Field: The Humanitarian Crisis in Ukraine. *Journal of Human Security.* 2015, Vol. 11, 1, pp. 27-33.

Seimas. 2022. *[The state budget 2022 of the Republic of Lithuania].* Vilnius, Lithuania : Seimas [Parliament of the Republic of Lithuania], 17 March 2022. Lietuvos Respublikos 2022 metu valstybes biudzeto ir savivaldybiu biudzetu finansiniu rodikliu patvirtinimo isakymo Nr. XIV-745 14 straipsnio pakeitimo istatymas. XIV-943.

—. 2022. *[The state budget 2023 of the Republic of Lithuania].* Vilnius, Lithuania : Seimas [Parliament of Republic of Lithuania], 22 November 2022. Lietuvos Respublikos 2023 metu valstybes biudzeto ir savivaldybiu biudzetu finansiniu rodikliu patvirtinimo istatymas. XIV-1556.

—. 2021. *National Security Strategy.* Vilnius, Lithuania : Seimas [Parliament of the Republic of Lithuania], 22 December 2021. Nutarimas, Del Lietuvos Respublikos Seimo 2002 m. geguzes 28 d. nutarimo Nr. IX-907 „Dėl Nacionalinio saugumo strategijos patvirtinimo“ pakeitimo. XIV-795.

Sheehan, Christopher J. 2015. Nonstandard Logistics Success in Unconventional Warfare. *Trade Journal.* 2015, Vol. 47, 6, pp. 22-28.

Shlapak, David A. and Johnson, Michael. 2016. Reinforcing deterrence on NATO’s eastern flank: Wargaming the defense of the Baltics. [Online] 2016. [Cited: 8 February 2023.] file:///C:/Users/Student/Downloads/RAND_RR1253.pdf.

Shynkarenko, Mariia. 2022. Communist and Post-Communist Studies: Compliant Subjects?: How the Crimean Tatars Resist Russian Occupation in Crimea. *The New School for Social Research.* 2022, Vol. 55, 1.

Skrypnik, Olga, et al. 2016. *The peninsula of fear: Chronicle of occupation and violation of human rights in Crimea.* [ed.] Tetiana Pechonchyk. Kyiv : KBC, 2016. p. 136. ISBN 978-966-2403-11-4.

Sliwa, Zdislaw. 2022. Poland as a front-line nation in the wake of Russian aggression in Ukraine. [ed.] Adres Saumets. *Putin's war in Ukraine. The background and anatomy of Russian aggression. Sõjateadlane [Estonian Journal of Military Studies].* 2022, Vol. 1.

State Forest Service. 2022. *Lietuvos misku rodikliai [Lithuania's forest data].* Kaunas : Valstybine misku tarnyba prie LR Vyriausybes [State Forest Service to the Government of Lithuania], 2022.

—. 2022. *Misku nuosavybe ir administracinis pasiskirstymas [Ownership and administration of forests].* Kaunas : s.n., 2022.

Statistics Department. 2022. *Leidinio „Lietuvos gyventojai“ pristatymas [The presentation of the report on Lithuania's population].* Statistics Lithuania, State Data Agency. Vilnius : Statistics Department of Lithuania, 2022.

—. 1974. *Lietuvos TSR kaimo gyvenamosios vietoves 1959 ir 1970 metais [Lithuanian TSR rural urbanized areas in the years of 1959 and 1970].* Vilnius : Centrine statistikos valdyba prie Lietuvos TSR Ministru tarybos [Central Statistics Department of Lithuanian TSR Minister Council], 1974. 0126.

Steiner, N. D., Berlinschi, R., Farvaque, E., Fidrmuc, J., Harms, P., Mihailov, A., Neugart, M. and Stanek, P. 2022. Rallying around the EU flag: Russia's invasion of Ukraine and attitudes toward European integration. *JCMS: Journal of Common Market.* 2022, Vol. 61, 2.

Stejskal, James. 2022. Bear Trap: Building a Pre-Conflict Underground Force to Resist the Future Enemy. *Journal on Baltic Security.* 2022, Vol. 8, 1.

Stringer, Kevin D. and Fiala, Otto C. 2019. The ROC (Resistance Operating Concept). *Special Warfare.* 2019, Vol. 32, 3.

Stringer, Kevin D. 2021. Survival in the Russian Occupied Zone. *Military Review.* 2021, Vol. 101, 4.

UNHR. 2022. *UN report details summary executions of civilians by Russian troops in northern Ukraine.* s.l. : United Nations Human Rights, Office of the High Commissioner, 2022.

United Nations. 2023. UN General Assembly calls for immediate end to war in Ukraine. *UN News. Global perspective Human stories.* [Online] UN, 2023. [Cited: 18 March 2023.] https://news.un.org/en/story/2023/02/1133847.

VOA. 2022. UK: Russia 'Killing Civilians It Now Claims as Its Own Citizens'. *Voice of America news.* 2022.

Watling, Jack. 2023. Russia Through the Kremlin’s Eyes. *RUSI.* 2023.

Yaffa, Joshua. 2022. The Captive City. *New Yorker.* 2022, 13.

Zabrodskyi, Mykhaylo, et al. 2022. *Preliminary Lessons in Conventional Warfighting from Russia's Invasion of Ukraine: February–July 2022.* London : Royal United Services Institute (RUSI), 2022.

Zdanavicius, Liudas and Statkus, Nortautas. 2020. Strengthening Resilience of Lithuania in an Era of Great Power Competition: The Case for Total Defence. *Journal on Baltic Security.* Journal on Baltic Security, 2020, Vol. 6, 2.

BEST ESSAY OF THE COMMAND SENIOR ENLISTED LEADER'S COURSE (CSELC)

MCPO Lars RAABE. The Implications of the Russian-Ukraine War to the Baltic Sea Region from a Maritime Perspective.

Introduction

The Baltic Sea represents a unique maritime environment, surrounded by NATO, EU member states and the Russian Federation. Access to the Baltic Sea is limited through the Danish Straits. The Baltic Sea Region is a central and focal point of cultural and economic exchange, closely tying NATO and EU member states. As one of the busiest seas in the world, it relies on the regional security, stability and freedom of movement. Former Soviet Union or Warsaw Pact nations Poland, Lithuania, Latvia and Estonia have chosen EU and NATO membership. EU members Finland and Sweden are currently in the process of becoming NATO members. The Baltic Sea is also a major trade route for the export of Russian petroleum.

From a naval warfare perspective, the Baltic Sea can be defined as “Confined and Shallow Waters” requiring refined means and skills, imposing operational limitations as well as the requirement for specific capabilities. Russian Naval presence consists of their Baltic Fleet, naval shipbuilding and service support as well as naval bases and extensive military underwater activities.

Russia’s war of aggression against Ukraine marks a turning point in European security and defence policy. Russia as an unpredictable actor has declared the West as its main adversary (Russia, 2021) and poses a serious threat to NATO, EU and its Baltic Sea Region.

NATO is reinforcing both its deterrence capability and defence posture, adapting its command-and-control structure (C2) and developing new defence plans. (TRANSCRIPT, 2021) (Daniel Hamilton, 2022)

This paper will argue that the Baltic Sea States should intensify their regional maritime coordination and C2 elements to complement NATO’s command structure and regional deterrence and defence planning. Additionally, the Baltic Sea States should concentrate on combining their relevant maritime warfighting capabilities.

Part I - The Baltic Sea's need for Security and Stability

Maritime security is of great importance for the Baltic Sea States. As one of the most frequented seas in the world, the Baltic Sea is an important lifeline for its neighbouring regions. Shipping supports the import and export as a basis for domestic trade, as well as for passenger transport and cruise tourism. The Baltic Sea may be geographically a marginal European sea, but in terms of security policy it affects the interests of the entire continent. In recent years, the Baltic Sea has grown in fundamental strategic importance. Like nowhere else, economic relations and security tensions meet in such a concentrated area. The Baltic Sea has now unfortunately become a focal point of NATO's northern and eastern flank due to President Putin's policy of aggression – highly militarized and with the constant potential of escalation between NATO and Russian forces. The stability of the Baltic Sea Region is crucial to securing essential sea links and communication lines in this extremely dynamic economic area, even if divided among several geopolitical blocks. (Foundation, 2021)

With the annexation of Crimea in 2014 by Russia and the invasion of Ukraine, Russia displays that it is impossible to integrate the world's biggest country into prevailing European security architecture as a responsible stakeholder. Putin clearly intents to destroy the cooperative security order in Europe and members of EU and NATO will need to prepare quickly for a long-term confrontation with Russia. Especially, the Baltic region is one of the areas where allied capabilities need strengthening in order to protect Estonia, Lithuania, Latvia and provide stability for the whole region. Often communicated, the Baltic Sea States need to strengthen regional maritime coordination as well as C2 willing to take responsibility for their own backyard and area of expertise.

Part II – Global Power Interests in the Baltic Sea Region

Russia: The Baltic Sea has always been of geopolitical and global interest. In terms of security, it seems that the western countries and Russia speak different professional languages and debate in parallel worlds resulting in dramatic effects on regional security. The main pattern with regards to Russia is no longer cooperation but confrontation. Russia's National Security Strategy declares the west as its main adversary, accusing the Alliance of encircling Russia.

31 August 2022, the Russian President signed a new naval doctrine. It states that the United States (US) and NATO are the "greatest Russian national security threats." Specifically, Washington's "strategic goal of dominating the world's oceans" and the "rapprochement of NATO's military infrastructure to the Russian borders" are named as dangers. Russia defines itself as a maritime superpower in the tradition of Peter the Great. In it, Russia names its own strategic areas of influence and underlines its will to defend national interests on all oceans, if necessary, by using military means.

Despite their focus on the Arctic and the Northeast Passage, the importance of the Baltic Sea access is mentioned as national security interest. The supply of the Kaliningrad exclave from St. Petersburg will be increasingly secured by sea lines in the future. This reflects the concern about a landside blockade of the Suwalki corridor by the west and increases the importance of Russia's sea lines of communication in the Baltic Sea. (Russia, 2022)

China: China's global political rise challenges established regional and global power relations while increasingly calling western ideas of order into question. The Baltic Sea region is for China strategically significant. It is one of the end points for the Belt and Road initiative aiming to connect Europe and Asia through infrastructure and trade with a potential link to their planned “Polar silk road” in the arctic to connect Asian and European shipping lanes. The investment of China in the Baltic Sea region has increased in recent years, corresponding with the overall growth in Chinese investment in Europe over the past decade. Beijing's policy of investing in and partially owning key European ports and technological infrastructure requires an economic or political response above all else. (Brattberg, 2019)

The biggest concerns, in the sense of security for the Baltic Sea region, are the increasing closeness between China and Russia, especially the military cooperation between the two states. The scope of Russian-Chinese military cooperation is still very limited and does not reflect a defined strategic commitment by both sides. In 2017, China deployed a destroyer, a frigate and a supply ship to the Russian exclave of Kaliningrad as part of an eight-day exercise. This was the first such military exercise in the Baltic Sea. (Ebbighausen, 2017)

Nevertheless, a growing convergence of interests and strategic coordination between China and Russia cannot be overlooked and doesn't apply to military and military-technical cooperation only. With great power competition between the US and China likely to intensify in the coming years, it is vital that Baltic Sea countries closely monitor broader geopolitical developments and pursue strategies aimed at protecting national interests. (Angela Stanzel, 2022)

The United States: The US National Defense Strategy (NDS) 2022 places greater focus on the support of partners and allies, particularly NATO. It also implies a bigger role for all allies going forward and support the US to meet its challenges and strategic goals, especially in the European area and its neighborhood. The US places its higher long term priority towards China and the Indo-Pacific than to Russia and Europe, even if they called Russia an "acute threat" in this document. (USA, 2022)

The Chief of Naval Operations US Navy (USN), Admiral Gilday, published an update of his Navigation Plan (NAVPLAN) on the 26 July 2022. Derived from the NDS, the NAVPLAN describes current challenges and fields of activity for further development of the USN. Geographically, eleven strategically relevant choke points are described by the USN, including the approaches and sea lanes to the Baltic Sea. To mention the Baltic Sea approaches as a choke point of strategic relevance underlines the continued interest in the Baltic Sea, despite an increasing threat, especially in the Indo-Pacific and the Arctic region. (USN, 2022)

Since NATO's foundation, Europe has relied on extended deterrence provided by its US ally. Europe needs the US far more than they need its European allies. One fundamental inequality remains, the US is able to protect itself if necessary. Europe does not have this autonomy. Europe must learn to replace the US as a security provider due to their increased focus on China and the Indo-Pacific region.

Reflecting the national and maritime strategies of the three global power states, the Baltic Sea remains an important and strategic area of interest. However, the focus of the global power states is shifting to the Arctic region and the Indo-Pacific. This requires and mandates the European countries of NATO and EU to take over more responsibility and enhance their forces. Recognizing regional expertise, the Baltic Sea States' navies must expand their close cooperation to reinforce regional and tactical

coordinated and led combat forces in order to enhance the ability to operate effectively, to deter, defend and deny, if necessary.

Part III – Finland and Sweden accession / Russia's trade routes and communication lines / The Russian Baltic Fleet / Strategic maritime challenges

With the accession of Sweden and Finland to NATO, the geography in the Baltic Sea region is fundamentally changing. Except for the exclave of Kaliningrad and the Bay of Saint Petersburg, the entire Baltic Sea is surrounded by NATO members. There are thousands of kilometers of coastline added to the NATO territory, which must be protected and defended, if necessary. The armed forces of Finland and Sweden are also adding capabilities that must be considered in future NATO planning. The Alliance will gain a greater strategic and operational depth in the region as well as the ability to exercise greater control of the maritime and air space in the Baltic Sea region.

Russia, which only controls 7% of the Baltic coast and divides its marine posture between the eastern end of the Gulf of Finland, Saint Petersburg and the isolated enclave of Kaliningrad, is in the least favorable geostrategic position. A significant portion of Russia's shipbuilding sector is based there and a third of its maritime trade passes via the Baltic Sea. Approximately 45% of the Russian sea trade is shipped over Saint Petersburg. (Solution, 2021) Russia is dependent on, but unable to control, all the lines of communication with Kaliningrad and the outside world. Control of the Baltic Sea would give Russia permanent access to Kaliningrad, protection for trade, depth for its air defence in the west and strategic depth for its nuclear forces on the Kola Peninsula. Since such a significant portion of Russia's maritime trade passes via the Baltic Sea, any significant disruption of energy export and trade would have considerably greater negative effects on the country's economy. (Laanemets, 2021)

Over the last years, Russia has strengthened its air and naval presence in the Baltic Sea. This process has been going on since Ukraine's Crimea was annexed by Russia. (Chang, 2021) The Baltic Fleet is a multiservice organization (fleet, naval aviation, motorised rifle and tank units, strategic air defence systems) with a mandate for the defence of the Saint Petersburg and Kaliningrad territory, but historically and culturally, it has been primarily a naval unit with the Baltic Sea as its primary theater of operations. As a result, the Baltic Fleet's function is intimately tied to how important the Baltic Sea

is to Russian national interests, including its economy. (Kjellén, 2021) Russia's Naval Forces are violating "territorial waters" and practicing "mock attacks" on NATO ships and bases during exercises. (Chang, 2021) These actions were supported by air defence systems and surface-to-surface missiles. Russia's exercise scenarios are designed offensively and focuses on the Baltic States, Poland, and Nordic nations. From the Kaliningrad Oblast, the territory of the adjacent NATO countries could easily come under fire by the Russian missile systems stationed there. Russia's anti-access/area denial (A2/AD) systems are also threatening these countries and NATO's ability to reinforce the Baltic allies by sea and air. With the use of these systems, together with Russian navy surface and submarine forces, electronic warfare, and cyber warfare, they may transform locations that are within these weapons' range into strategically and operationally isolated "bubble" zones. (Lasconjarisa, 2016)

However, the efficacy of Russia's A2/AD capabilities has often been overestimated. Even if countering A2/AD poses a challenge and is very difficult with a potential risk of time loss and loss of capabilities (Dalsjö, 2019), the Baltic Sea states and NATO would be capable of dealing with it. Russia's Baltic Fleet is not designed for decisive sea battles and does not have the necessary quantity and quality of its ships and boats to undertake sustained conventional naval combat operations. (Lokshin, 2018) There are also signs of structural weaknesses regarding equipment, training and operating the fleet. (Lendon, 2018) Therefore, Russia lacks the resources to dominate the Baltic Sea while the naval forces of NATO members and partners such as Sweden and Finland, in conjunction with its land based air and missile defence forces, are clearly superior in the Baltic Sea region.

Most likely, hybrid warfare is one way of Russia dealing with geopolitical adversaries. The Baltic Sea offers a wide range of opportunities for hybrid damages from a maritime domain. Port infrastructure, pipelines, or undersea communication cables have all been identified by Russia as potential ways to "split NATO", challenge the resilience of Europe and test its response, while still ensuring plausible deniability. (Heinrich Lange, 2019) The Baltic Sea, including its underwater and seabed infrastructure, continues to be the major communication line especially for nations with limited land connectivity to the rest of the western world. It needs to be protected of the surrounding states. The Baltic Sea nations should view these hybrid maritime threats as shared issues that are best solved via cooperation.

Part IV – NATO's Military Strategic Environment

NATO updates its posture with regards to its Deterrence and Defence of the Euro-Atlantic Area (DDA, 2022) (Vincent, 2022), evaluates its C2 structure and develops new defence plans -SACEUR's AOR-wide Strategic Plan (French, 2022). Regional plans will provide the operational implementation of future Alliance deterrence and defence posture, where "each NATO member is understood to be looking at placing more of its own forces in a greater state of readiness to defend a particular area of NATO territory" (Brzozowski, 2022). What applies to the Joint Force Commands (JFC) since the launch of the Readiness Action Plan (RAP, 2022) – moving away from NATO Response Force rotations to a fixed regional responsibility – should also be the future for certain tactical command elements, including the maritime domain. This regional approach to C2 has manifested itself already in the land domain with the Multinational Corps North East set up as a regional Land Component Command (MNCNE, 2022). In addition, the changes to NATO's geography in the Baltic Sea region and the Northern Flank land borders after the accession of Finland and Sweden will most likely call for an adjustment of defence planning.

Allied Maritime Command (MARCOM) acts on the operational level as the principal maritime advisor to the Supreme Allied Commander Europe (SACEUR) and as Maritime Theater Component Commander (MTCC) for NATO maritime operations during Baseline Activities and Current Operations (BACO). The MTCC provides a 360-degree maritime focused situational awareness and connectivity throughout the entirety of SACEUR's Area of Responsibility. Throughout a crisis in the Baltic Sea region, MARCOM will hand over its MTCC responsibility to a JFC, most likely the JFC Brunssum, a land-heavy headquarters. (Heinrich Lange, 2019) Due to the 360-approach, MARCOM lacks regional expertise, particularly in the Baltic Sea and its complex operating environment. MARCOM's initiative, to establish a Baltic Sea Regional Maritime Coordination Function (BMCF) with regional expertise maintaining close coordination with regional navies, but without command function, has not been achieved yet. (Heinrich Lange, 2019)

Considering there is no regional maritime headquarters to generate local knowledge of the Baltic Sea in times of peace and to command activities during times of crisis and

conflict, the idea to establish a multinational regional Baltic Maritime Component Command (BMCC) as part of the Framework Nation Concept, collocated with the respective national Maritime Operations Centre (MOC) and available to NATO, is desired by the Baltic Sea states at the navy level and would continue the idea of a BMCF. Showing presence, coordinating national forces, creating and conducting regional exercises will become an increasing permeant task in addition to the possibility to be augmented to provide C2 for regional maritime NATO operations in time of crisis and war. (Heinrich Lange, 2019). Germany as well as Poland have offered to take over the lead of the BMCC responsibilities. Both nations are in their planning and establishment process with their respective MARFORs and are competing each other, challenging the Baltic Sea maritime “unity of effort”. (Swistek, 2020)

The need for regional maritime coordination, C2, as well as more detailed maritime images and situational awareness, is strongly supported and articulated by nations in light of the current security situation, the Russian Federation's aggression, and Finland and Sweden's applications to join NATO. It seems that the Baltic Sea Nations have a common desire to develop such a capacity, which runs parallel to NATO's concept for a Regional Maritime Coordination Function.

Conclusion

The Baltic Sea stands out for its strong economic growth, high volume of marine traffic, undersea pipelines and cables, power lines, offshore wind farms, LNG terminals, and many small- and medium-sized ports with important IT infrastructure. For overall stability as well as the region's economic development, the Baltic Sea region's peace and security are crucial to all surrounding states, including Russia.

For NATO’s defence efforts, the Baltic Sea is crucial when it comes to reinforcement and resupply. The use of the Baltic Sea for operations of NATO naval forces must always be ensured, at all times.

Russia remains a “dangerous troublemaker” in the Baltic Sea and will continue its provocative and aggressive behavior in addition to their extensive underwater activities as part of their hybrid warfare. Maintaining open lines of communications between Kaliningrad and Saint Petersburg will be their strategic goal in a conflict.

Since the focus of the global power states has shifted to other regions in the world, Europe and especially the Baltic Sea states must take over more responsibility to protect and defend their own “backyard”. In the maritime domain, a more coherent regional approach needs to be established to not only concentrate on deterrence, but also on relevant warfighting capabilities. It is important to see the Baltic Sea as a global shared battlespace for all the neighboring nations when it comes to maritime control. Regional coordination, cooperation and leadership needs to be strengthened and reinforced in order to use all operational capabilities. The Baltic Sea navies will play a crucial role in opposing Russia's maritime hybrid warfare.

Since the Alliances decision-making process will always be slower than Russia’s, NATO’s command structure needs to be complemented by regional coordination and C2 elements. A NATO Regional Maritime Headquarter for the Baltic would be perfect to play a significant role at the tactical level in the future. Day-to-day coordination will provide added value to MARCOM and could provide regional coordination of forces and respective activities on a permanent basis in support of national and NATO entities. Tactical cooperation, information exchange and mutual understanding would be greatly facilitated by common activities throughout the year and prove regional maritime readiness at an early stage, in peacetime and on “road to crisis”, to maintain quick decision-making and rapid reaction in the case of any aggression.

“Knowing is not enough, we must apply. Willing is not enough, we must do.”
– J.W. Goethe

Bibliography

Putins Ostseeflotte. Die wahre russische Gefahr lauert in einem anderen Meer. **Lokshin, Pavel. 2018.** s.l. : Die Welt , 2018.

Angela Stanzel, Markus Karim. 2022. *Der Aufstieg Chinas.* s.l. : SWP, 2022.

Brattberg, Erik. 2019. *Chinese Investment in the Baltic Sea Region.* 2019.

Brzozowski, Alexandra. 2022. *NATO to massively increase high-readiness forces to 300,000.* s.l. : EURACTIVE.com, 2022.

Chang, Felix K. 2021. *Crowded Pond: NATO and Russian Maritime Power in the Baltic Sea.* s.l. : BALTIC BULLETIN: Foreign Policy Research Institute, 2021.

Dalsjö, Berglund and Jonsson. 2019. *Bursting the Bubble. Russian A2/AD in the Baltic Sea Region, Capabilities, Countermeasures, and Implications.* 2019.

Daniel Hamilton, Hans Binnendijk. 2022. *One Plus Four: Charting NATO's Future in an Age of Disruption, NATO Task Force Report.* s.l. : www.transatlantic.org, 2022.

DDA, NATO. 2022. NATO Homepage. *DDA.* [Online] 2022. https://www.nato.int/cps/en/natohq/topics_133127.htm.

Ebbighausen, Rodion. 2017. *China, Russia join forces.* s.l. : DW.com, 2017.

Foundation, The Jamestown. 2021. *Baltic Sea Security.* 2021.

French, Julian Lindley. 2022. *NATO's Clint Eastwood Doctrine.* s.l. : https://aspeniaonline.it/natos-clint-eastwood-doctrine/, 2022.

Heinrich Lange, Bill Combes, Tomas Jermalavicius, Tony Lawrence. 2019. *To the Seas Again - Maritime Defence and Deterrence in the Baltic Region.* s.l. : RKK ICDS, 2019.

Kjellén, Jonas. 2021. *The Russian Baltic Fleet.* s.l. : Swedish FOI, 2021.

Laanemets, Ott. 2021. *Sea Power in the Baltic Sea.* s.l. : Sõjateadlane (Estonian Journal of Military Studies), 2021.

Lasconjarisa, Fruehling and. 2016. *NATO, A2/AD and the Kaliningrad Challenge.* s.l. : Survival, Global Politics and Strategy, 2016.

Lendon, Brad. 2018. *Russia's navy parade: Big show but how much substance?* s.l. : CNN, CNN, 2018.

Lokshin, Pavel. 2018. *Putins Ostseeflotte. Die wahre russische Gefahr lauert in einem anderen Meer.* s.l. : Die Welt , 2018.

MNCNE. 2022. Homepage MNC-NE. [Online] 2022. https://mncne.nato.int/about-us/mission/the-five-ws.

RAP, NATO. 2022. NATO Homepage. *Readiness Action Plan.* [Online] 2022. https://www.nato.int/cps/en/natohq/topics_119353.htm.

Russia. 2022. *Maritime Doctrine of the Russian Ferderation.* 2022.

—. 2021. *National Security Strategy (NSS2021).* 2021.

Solution, The World Integrated Trade. 2021. https://wits.worldbank.org/CountryProfile/en/Country/RUS/Year/LTST/TradeFlow/Import/Partner/by-country/Product/16-24_FoodProd. [Online] 2021.

Swistek, Göran. 2020. *Abschreckung und Verteidigung im Ostseeraum.* s.l. : SWP German Institute for International and Security Affairs, 2020.

TRANSCRIPT. 2021. *GEN Wolters remarks at the Atlantic Council, Competition on Deterrence in Europe Event .* s.l. : US European Command and Puplic Affairs, 2021.

USA. 2022. *National Defence Strategy.* 2022.

USN, CNO. 2022. *CNO NAVPLAN 2022.* 2022.

Vincent, Brandi. 2022. *NATO refining domain-specific 'family of plans' to guide allies' cooperation in future contingencies.* s.l. : DefenseScoop, 2022.

WO Murugesvaran SUBRAMANIAM. Russia and Iran – The Rapprochement.

"Putin's desire to dismantle what remains of democracy and replace it with a jingoist, messianic, Slavic concoction … makes him and his Russia an ideal ally, and role model, for Iran's pseudo-totalitarian antimodern regime"
(Milani, 2007)

Rapprochement: (especially in international affairs) a situation in which the relationship between two countries or groups of people becomes friendlier after a period during which they were enemies.
Oxford English Dictionary

Introduction

Russia and Iran have been commercially and militarily active for centuries. Their relationship dates back to the 8th century and their power in the region has been fairly balanced. Russia and Iran have fought wars between themselves and they have also managed to regain a diplomatic relationship for the stability of the Caucasus. In the 80s the Soviet Union supplied large amounts of weapons to Iran during the Iran-Iraq war especially when the USA imposed an arms embargo on Iran and supported Saddam Hussein (Friedman, 1993). The USA and UK provided arms and intelligence support to Iraq during the war thus solidifying the relationship between the Soviet Union and Iran (Rubinstein, 1981). In the early 90s, the fall of the Soviet Union saw a different relationship between Russia and now the Pariah state Iran. Ayatollah Khamenei assumed the office of the Supreme Leader of the Islamic Republic on June 4, 1979. He witnessed the fall of the Soviet Union and the influence USA and the UK had in its demise (Davar, 2021). Iran endured a coup d'état in 1953 orchestrated by the Central Intelligence Agency in Operation Ajax, where the USA assisted in the overthrow of the democratically elected Prime Minister Mohammad Mossadegh in favour of strengthening the monarchical rule of the Shah, Mohammad Reza Pahlavi. Ayatollah Khamenei did not want Iran to be influenced by the West and suffer a similar fate as the Soviet Union (Davar, 2021). These western influences have inadvertently coagulated Russia and Iran's relationship.

This paper aims to examine the relationship between Russia and Iran. This study will consist of four parts. The first gives an overview of the history of Russia and Iran's affiliation. The second part will provide the current partnership between these two Nations. The third/fourth part will examine the strategic versus tactical influences Russian and Iran bring to the instability of the world order and draw on the current war in Ukraine. The final part will conclude this paper.

History

The rapprochement between Russia and Iran dates back to the 8th century, there were commercial exchanges (Therme, 2012.) between these two nations. In 1521, The Grand Duchy of Moscow and the Persian Empire (Iran) officially commenced trading, with the Safavids in the power (Newman, 2006). Safavid Shah Ismail I sent an envoy to visit Czar Vasili III. This relationship continued until the Russo-Persian war from 1651-53 when Russia had to concede to the Persians in the North Caucasus. After the war, peace reigned for many decades, but the Safavid state's decline and the fall of Shah Sultan Husayn saw the ascent of Imperial Russia. Iran lost significant influence in the region as Imperial Russia became influential in the region and their opposing ambitions for influence on a changeable frontier, and the Caucasus projected Russian-based dynasties have bothered relations between the two countries.

Whilst both countries continued their relationship, there has always been competition in the region. Russia and Iran always competed for resources and land in the Caucasus. During the Cold War, Russian-Iranian relations were predisposed by the worldwide alignment of forces in a bipolar geopolitical setting. Associated with the West, Iran faced its Soviet neighbour across the East-West philosophical impasse. While the Soviet Union was seen by the world as the Black Bear (Stilwell, 2022) with nuclear weapons and could start World War III. Iran projected a modern western cosmopolitan that was full of culture and exhilaration for the West. The rich and famous swarmed Iran’s capital. Iran accepted USA and UK’s major investments and the rally toward modernism overlapped with Ayatollah Khomeini’s exile to Najaf in 1964 (Niknejad, 2014), and the assassination of the secular Prime Minister Hassan Ali Mansour just a few months later. And for a period until the beginning of the revolution in 1979, the East and West coexisted in seeming harmony.

The 1979 revolution saw the ousting of King Shah Mohammad Reza Pahlavi and the return of Ayatollah Ruhollah Khomeini, this change in leadership would have long-lasting and far-reaching implications. The Islamic Revolution changed Iran in a new way, it is now actively eradicating all Western ideologies. The United States and the Soviet Union were both maligned in Iran's "neither East nor West" revolutionary worldview. However, Tehran's confrontational foreign policy transformed into a more

pragmatic approach as the realities of international relations and domestic challenges blunted the country's militant mood. Iran finally decided to improve relations with the "lesser Satan" (Shimon Shapira, Daniel Dinker, 2007) and the Soviet Union-Iran rapprochement began.

Russia and Iran's current relationship status

The Russian involvement in September 2015 provided pivotal air power to Syrian and Iranian-backed ground forces, intensifying Bashar al-Assad's territorial control and solidifying the regime's hold on power through analogous diplomatic efforts (Ramani, 2021). Throughout the course of the Syrian Civil War, standardised military and political interactions fortified the Russia-Iran relationship while contributing to greater coherence between Moscow and Tehran (Grajewski, 2021). Although, Russia was cautious about Iranians' intentions in Syria and its long game in the region. Russia eventually accepted the requests by General Qassem Soleimani of the Islamic Revolutionary Guard Corps (IRGC) Quds Force to assist in deploying Iran's ground forces. Many scholars believe that the Syrian Civil War was the turning point for Russia's influence in the Middle East and North Africa (MENA) region. This conflict also saw the Russia-Iran relationship strengthened because of the USA and UK's involvement in Syria.

Syria became the substratum of the Russia-Iran relationship, it also fortified Iran's view of their partnership especially when the West imposed further sanctions when Donald Trump became the 45th President of the USA (Stefan Reisinger, Kim Caine, Katie McDougal, Wenda Tang, 2020). The association further bonded when Russia invaded Ukraine on the 24th of February 2022 (Taylor, 2022). The illusion of isolation between Pariah states does exist (Myers, 2012) and this is what bonds them further. When Nations are pushed out from the mainstream they tend to share a common enemy and develop a convergence interest. Professor Abbas Milani of the University of California stated that "Putin's desire to dismantle what remains of democracy and replace it with a jingoist, messianic, Slavic concoction … makes him and his Russia an ideal ally, and role model, for Iran's pseudo-totalitarian antimodern regime" (Milani, 2007).

Russia and Iran: Tactical vs Strategic

Iran's relationship with Russia has predominantly been tactical in the early post-Soviet era, their relationship has fluctuated during this period. It was generally influenced by who is in power in Russia and Iran; and it also depended on the external influences or pressures asserted by the West, especially the USA. Iran's former President Mahmoud Ahmadinejad (2005–13) strived to do so as part of his 'Look East' foreign policy. Since the relations with the West were strained under his administration facilitated the consolidation of Iran's relationship with Russia, which shares, in particular, Iran's anti-Americanism and its desire to side-line the US in the Middle East. By contrast, moderates and reformists largely prioritise the improvement of Iran's ties to the West, giving rise to a perception of the Tehran–Moscow axis as tactical and issue-based.

However, since 2015 Iran's relationship with Russia has been strategic in nature (Studies, 2020). Russia and Iran with a collective mindset proceed to influence the MENA through proxy wars and nuclear programmes. The withdrawal of the USA and UK from Afghanistan and Iraq has increased their sway in the region, the Persian Gulf has inevitably created a power vacuum that has been filled by Russia and Iran working in collaboration (Seth Cropsey, Gary Roughead, 2019). The support of proxy war (Brands, 2021) in Yemen, Iraq and other regional disputes has seen Iran flourish under the tutelage of General Soleimani. Russia's support in providing Iran with weapons and ammunition has only strengthened its position in the Caucasus.

Russia and Iran: Ukraine

The relationship between Russia and Iran has expanded since the invasion of Ukraine in February 2022. Russia and Iran's partnership is evolving into a strategic outlook and many Senior Russian and Iranian leaders have met frequently in recent months to boost cooperation and sign economic and military agreements. Moscow and Tehran have long collaborated when their interests have united, especially in trying to reduce USA's influence in the Middle East, but their recent arrangements emphasised more determined efforts to reinforce their partnership. Presidents Vladimir Putin and Ebrahim Raisi have spoken many times (Sinaee, 2022) since the invasion began—more than either country has engaged with other world leaders. Putin's visit to Tehran in July 2022, marked his first foreign travel outside the territory of the former Soviet

Union since the war began (Guy Faulconbridge, Parisa Hafezi, 2022). These exchanges reflect a deepening and potentially more balanced relationship wherein Russia is no longer the dominant party. This enterprise will likely test the USA and UK interest in Europe, the Middle East, Asia and around the globe.

After seven years of the annexation of Crimea and the invasion of Ukraine, Russia finds itself in a battle that it finds difficult to win. It is unlikely that Russia will emerge victorious (Gressel, 2022) without the assistance of an ally. While Tehran initially acknowledged Moscow's rationale for the invasion and attempted to show its political support in the United Nations General Assembly (Nasr, 2022), Iran has remained cautious about fully supporting Russia's war efforts, even as it seeks to benefit from the resulting trade and security opportunities. However, Tehran had a change of mind; Iran embraced Russia after the West decided to rebuff Russia's intention to expand its territories. Russia has spent years sending arms to Iran but since the war in Ukraine, the arms traffic is somewhat reversed in recent times. Russia's predicament in Ukraine has prompted Moscow to turn to Tehran for support, Iran immediately stepped up as the major sponsor of precision-guided arms to provision Russia's war in Ukraine (Marcus, 2022).

Iran has deepened its commitment to supplying arms for Russia's assault on Ukraine by agreeing to provide a batch of medium-range missiles, as well as large numbers of cheap but effective drones, according to US and Iranian security officials Iran has been supplying Russia with its kamikaze drones (Cleverly, 2022). The Iranians have also been supplying Russia with two short-range missile systems capable of striking targets at distances of 300km and 700km. Whilst, Iran denied selling missile systems and drones to Russia; the downed drones in Ukraine do imitate Iranian technology.

Tehran's military support is already making its deadly mark on the war, but the geopolitical consequences extend much further. By intensifying its support for Russia's imperial attempt to defeat Ukraine, Iran hopes to expand its agenda in the Middle East. Tehran will likely seek to influence the strengthening Russo-Iranian partnership into arms deals from Moscow while using lessons learned from the Ukrainian battlefield to perfect Iranian drone and missile capabilities. At the same time, the regime in Iran likely hopes that fuelling the crisis in Ukraine will further distract the West from confronting

Iran's pursuit of domination in the Middle East (Eugene Rumer, Richard Sokolsky, 2021).

The rapprochement benefits both nations, Iran is given an opportunity to showcase its military armament – Shahed 136s (Iran's homegrown drone) and if these drones tilt the balance in the Ukrainian war. There is an assumption that non-mainstream countries that are currently struggling to deal with the West due to sanctions or embargos will look towards Iran to provide them with drones and other military armaments tested in Ukraine. Russia on the other hand gets dozens of drones at a reasonable cost and Putin is supported by ground forces that do not use similar military tactics as the European Nations (Ostovar, 2018). Russia has an ally that understands sanctions and restrictions. Since Iran has managed to survive for decades under these conditions, it will be able to assist Russia to navigate the ostracised world that it is in now.

Conclusion

At a June 2019 Shanghai Cooperation Organization summit, when Russian President Vladimir Putin met with Iranian President Hassan Rouhani, he remarked that the relations between the two countries were "multifaceted" and "multilateral." The two countries have continued developing their ties despite tightened sanctions. The rapprochement between Russia and Iran exists due to their political standing in the multifaceted world that the West has placed them. Ruslan Pukhov, Director of the Centre for Analysis of Strategies and Technologies from Russia at the CSIS Conference in Washington DC in September 2019 on the topic of Russia-Iran: Agreements and Disagreements supported this comment. He went further to support this claim by stating that, even though Iran's ideology is somewhat different to Russia's; they will always seek an alliance with other nations that are vilified by the West, especially the USA.

Whilst this cooperation seems equally balanced, Iran appears to benefit a great deal from Russia. Russia supported Iran when former US President Donald Trump pulled out of the 2015 nuclear agreement – the Joint Comprehensive Plan of Action (JCPOA). Iran already runs one of Russian- built nuclear power reactors at Bushehr and with the latest talk about US waivers (International, 2022) Russia and Iran will benefit from Biden's administration. The report claims that Russia manages to benefit

from $10 Billion from the nuclear deal and Iran gets its nuclear capability. Russia has also launched Iran's imagery satellite, Khayyam, from Baikonur Cosmodrome in Kazakhstan. This has strengthened their strategic relationship.

However, a study done by The Copenhagen-based Alliance of Democracies Foundation's 2022 Democracy Perception Index notably determined that 50% of Iranian people hold a negative perception of Russia, while only 15% expressed very or somewhat positive views of that country.

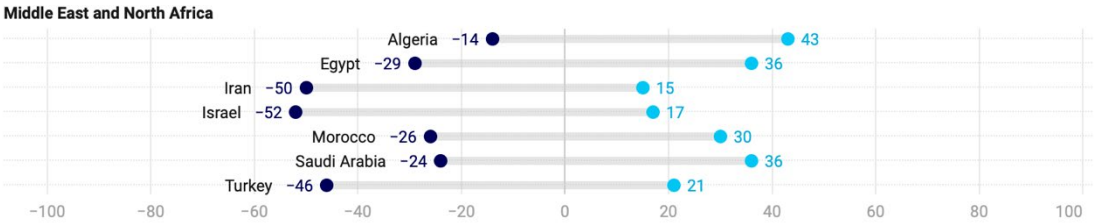


Figure 1: 2022 Democracy Perception Index (Kafura, 2022)

Conversely, Russia and Iran rule their population in a similar fashion. They might have a different ideology but they have been oppressing their population for decades (McDaniel, 2004). Irrespective of the populace's view of Iran, the Islamic Republic's relationship is very unlikely to change their relationship with Russia and Putin's desperate need for weapons, troops and funding will see Russia in bed with Iran for some time to come. These two nations will be the thorn to stability in the Middle East region and Iran's support of Russia in Ukraine deepens the geo-political issues. Russian and Iran's rapprochement will continue until the West decides to accept Iran and assist in a controlled nuclear program, this in return will leave Russia out in the cold without an ally to support Putin's egocentrically (Lloyd, 2022) view of the world politics.

Bibliography

Brands, Hal. 2021. Russian and Iranian Proxy Forces Are Baffling the US. *Bloomberg Opinion.* [Online] 22 July 2021. [Cited: 26 October 2022.] https://www.aei.org/op-eds/russian-and-iranian-proxy-forces-are-baffling-the-u-s/.

Cleverly, The Rt Hon James. 2022. UK sanctions Iran over kamikaze Russian drones. *Foreign, Commonwealth & Development Office.* [Online] 20 October 2022. [Cited: 24 October 2022.] https://www.gov.uk/government/news/uk-sanctions-iran-over-kamikaze-russian-drones.

Davar, Faramarz. 2021. Iran and Russia, Part I: What Khamenei Took From the Collapse of the Soviet Union. *Iranwire.* [Online] 1 November 2021. [Cited: 16 October 2022.] https://iranwire.com/en/special-features/70676/.

—. 2021. Iran and Russia, Part I: What Khamenei Took From the Collapse of the Soviet Union. *Iranwire.* [Online] 1 November 2021. [Cited: 16 October 2022.] https://iranwire.com/en/special-features/70676/.

Eugene Rumer, Richard Sokolsky. 2021. Grand Illusions: The Impact of Misperceptions About Russia on U.S. Policy. *Carnegie Endowment for International Peace.* [Online] 30 June 2021. [Cited: 23 October 2022.] https://carnegieendowment.org/2021/06/30/grand-illusions-impact-of-misperceptions-about-russia-on-u.s.-policy-pub-84845.

Friedman, Alan. 1993. *Spider's Web: The Secret History of How the White House Illegally Armed Iraq.* s.l. : Bantam Books, 1993.

Grajewski, Nicole. 2021. The Evolution of Russian and Iranian Cooperation in Syria. *Center for Strategic and International Studies.* [Online] 17 November 2021. [Cited: 26 October 2022.] https://www.csis.org/analysis/evolution-russian-and-iranian-cooperation-syria.

Gressel, Gustav. 2022. Mob unhappy: Why Russia is unlikely to emerge victorious in Ukraine. *European Council on Foreign Relations.* [Online] 21 October 2022. [Cited: 26 October 2022.] https://ecfr.eu/article/mob-unhappy-why-russia-is-unlikely-to-emerge-victorious-in-ukraine/.

Guy Faulconbridge, Parisa Hafezi. 2022. Putin forges ties with Iran's supreme leader in Tehran talks. *Reuters.* [Online] 20 July 2022. [Cited: 26 October 2022.] https://www.reuters.com/world/putin-visits-iran-first-trip-outside-former-ussr-since-ukraine-war-2022-07-18/.

International, Iran. 2022. *Russia To Get $10 Billion For Iran Nuclear Plant With US Waiver - Report.* Tehran : International, Iran, 2022.

Kafura, Craig. 2022. *2022 Democracy Preception Index.* Chicago : Chicago Council on Global Affairs, 2022.

Lloyd, John. 2022. How Valdimir Putin view the world. *The New Statesman.* [Online] The New Statesman, 29 July 2022. [Cited: 26 October 2022.]

https://www.newstatesman.com/world/europe/2022/07/how-vladimir-putin-views-world.

Marcus, Jonathan. 2022. Ukraine war: Growing Russia-Iran ties pose new dangers. *BBC News.* [Online] 21 October 2022. [Cited: 26 October 2022.] https://www.bbc.co.uk/news/world-middle-east-63328274.

McDaniel, Tim. 2004. *Autocracy, Modernization, and Revolution in Russia and Iran.* s.l. : Princeton University Press, 2004.

Milani, Abbas. 2007. Russia and Iran: An Anti-Western Alliance? *ProQuest.* [Online] October 2007. [Cited: 26 October 2022.] https://www.proquest.com/openview/51280e53a38a8e40ab307569b1b27177/1.pdf?pq-origsite=gscholar&cbl=41559.

Myers, Brian. 2012. *Cleanest Race, The : How North Koreans See Themselves - and Why It Matters.* New York : Melville House Publishing, 2012. 1935554344.

Nasr, Vali. 2022. The War in Ukraine and Its Impact on Russia-Iran Relations. *Middle East Institute.* [Online] 26 May 2022. [Cited: 22 October 2022.] https://www.mei.edu/events/war-ukraine-and-its-impact-russia-iran-relations.

Newman, Andrew J. 2006. *Safavid Iran: Rebirth of Persian Empire.* s.l. : IB Tauris, 2006.

Niknejad, Kelly Golnoush. 2014. From the archives: Iran in the 1960s - in pictures. *The Guardian.* [Online] 10 September 2014. [Cited: 10 October 2022.] https://www.theguardian.com/world/iran-blog/gallery/2014/sep/10/iran-swinging-sixties-in-pictures.

Ostovar, Afshon. 2018. The Grand Strategy of Militant Clients: Iran's Way of War. *Taylor & Francis Online.* [Online] 17 October 2018. [Cited: 27 October 2022.] https://www.tandfonline.com/doi/abs/10.1080/09636412.2018.1508862.

Ramani, Samuel. 2021. Russia and Iran in Syria: Military Allies or Competitive Partners? *London School of Economics.* [Online] April 2021. [Cited: 26 October 2022.] https://blogs.lse.ac.uk/mec/2021/07/03/russia-and-iran-in-syria-military-allies-or-competitive-partners/.

Rubinstein, Alvin Z. 1981. *The Soviet Union and Iran under Khomeini.* s.l. : International Affairs (Royal Institute of International Affairs 1944-), 1981. Vols. 57, No. 4.

Seth Cropsey, Gary Roughead. 2019. A U.S. Withdrawal Will Cause a Power Struggle in the Middle East. *Foreign Policy.Com.* [Online] 17 December 2019. [Cited:

26 October 2022.] https://foreignpolicy.com/2019/12/17/us-withdrawal-power-struggle-middle-east-china-russia-iran/.

Shimon Shapira, Daniel Dinker. 2007. Iran's Second Islamic Revolution: Strategic Implications for the West", Iran, Hezbollah, Hamas and the West: A New Conflict Paradigm for the West. *Jerusalem Centre for Public Affairs - Iran, Hizbullah, Hamas and Global.* [Online] 2007. [Cited: 13 Oct 2022.] https://jcpa.org.

Sinaee, Maryam. 2022. Iran Says Determined To Boost Ties With Russia 'At All Levels'. *Iran International.* [Online] 16 September 2022. [Cited: 26 October 2022.] https://www.iranintl.com/en/202209160361.

Stefan Reisinger, Kim Caine, Katie McDougal, Wenda Tang. 2020. Increased US sanctions on Iran. *Norton Rose Fulbright.* [Online] 17 January 2020. [Cited: 26 October 2022.] https://www.nortonrosefulbright.com/en-us/knowledge/publications/7b2febfd/increased-us-sanctions-on-iran.

Stilwell, Blake. 2022. How One Black Bear Almost Set Off World War III During the Cold War. *Military.Com.* [Online] 2022. [Cited: 26 Oct 2022.] https://www.military.com/off-duty/how-one-black-bear-almost-set-off-world-war-iii-during-cold-war.html.

Studies, The International Institute for Strategic. 2020. *Iran's Networks of Influence in the Middle East.* s.l. : Routledge, 2020. 9780860792185.

Taylor, Adam. 2022. Russia's attack on Ukraine came after months of denials it would attack. *The Washington Post.* [Online] 24 February 2022. [Cited: 20 October 2022.] https://www.washingtonpost.com/world/2022/02/24/ukraine-russia-denials/.

Therme, Clement. 2012.. *Relations between Tehran and Moscow, 1979-2014.* Paris : University Press, 2012.