



AD SECURITATEM

THE BEST ESSAYS BY COURSE PARTICIPANTS
AT THE BALTIC DEFENCE COLLEGE

ACADEMIC YEAR 2023/2024



TABLE OF CONTENTS

FOREWORD	3
BEST ESSAYS OF THE JOINT COMMAND AND GENERAL STAFF COURSE	4
OŁĘGS BOKŠE. Does Latvia, as a Host Nation, have the appropriate land transport infrastructure developed to allow the deployment of division-size NATO forces?	5
VIKTORAS BUIVA. The Fourth Imperialistic Wave Inside of Russia and Options for Sustainment.	23
TAAVI KAROTAMM. Is Estonia Ready to Involve Unorganized Support from Civil Population to National Defence as has Ukraine?	44
FELIX KESSERWAN. Equal Opportunity in the Armed Forces: A Case for Meritocratic Reforms	63
IMANTS KLEINBERGS. Critical Infrastructure Protection System And Resilience in Latvia	81
ZOIA KURTANIDZE. Can the Feminization of Leadership Improve National Security?	100
KAURI RAJU. What are the organisational outcomes from the relationship and the implications between leadership, management, and command?	120
LAURYNAS SINICA. Application of doctrinal special operations warfare during the war in Ukraine and its adaptation to contemporary military conflicts	154
KEVIN TEULADE. Russian Information Warfare in Estonia – A Case Study	175
BEST ESSAY OF THE HIGHER COMMAND STUDIES COURSE (HCSC)	202
MAREK BIALOBRZESKI. The reason behind Russia’s invasion of Ukraine?	203
COL MIROSLAV BORSUK. Technological Evolution and the Perception of Hybrid Warfare in Contemporary Conflicts	218
LIIVI TURK. What should be a successful strategy for a small state. Example of Estonia.	264
VILMANTAS VALANTINAS. Relations between Russia and China in the face of Russia-Ukraine war”	282
BEST ESSAY OF THE COMMAND SENIOR ENLISTED LEADER’S COURSE (CSELIC).	300
JANE ANDERSEN. Danish strategic challenges in the Baltic Sea after NATO’s expansion with Finland and Sweden.	301
BRIEFING NOTE FOR THE ARGUMENTATIVE ESSAY PRESENTATION PANEL	313

FOREWORD

This issue of *Ad Securitatem* features the best essays from the courses of JCGSC, CSC, HCSC, and CSEL written during the academic year 2023/2024. These essays received high valuations from their readers and can enrich the understanding of various strategic and operational issues in the Baltic Sea region, as well as touch upon leadership and military innovations.

We would also like to acknowledge some works that are not published in the current edition, as they are being reworked into academic journal articles. These include the work by Ms. Laura Gūtmane, HCSC 2024, entitled 'Is More Forward Allied Presence the Answer? From Deterrence to Containment: Strategy on Russia for Europe and the Baltic States'; LTC Uku Arold, HCSC 2024, entitled 'Cyber Power in Resistance Operations: Enhancing Security and Effectiveness'; and Maj. Andres Ojalt, JCGSC 2023/2024, entitled 'Are Estonian Preparations Sufficient to Support Resistance Operations in the Event of Partial or Full Occupation?'. A special mention goes to a paper titled 'The New Face of Battle: The Psychological Implications of a Future Cyber War', that is not included in this collection by the author's choice.

We extend our gratitude to the faculty members who acted as supervisors, guiding these students in their academic and professional writing endeavours. Their dedication has contributed to the quality of this collection.

BEST ESSAYS OF THE JOINT COMMAND AND GENERAL STAFF COURSE



OĻEGS BOKŠE. Does Latvia, as a Host Nation, have the appropriate land transport infrastructure developed to allow the deployment of division-size NATO forces?

Introduction

By joining the North Atlantic Treaty Organization (NATO) in 2004, Latvia declared its orientation towards Western democracies and showed its desire for collective defence within the Euro-Atlantic security structures. Contemporary global security has been worsening since that time because of Russia's aggressive foreign politics implementation in the form of military actions, such as the 2008 Russo-Georgian war, annexation of Crimea in 2014, and the ongoing Russo-Ukrainian war. Russia's full-scale invasion of Ukraine in 2022 proved President Putin's ambition to restore the Russian empire. In this Russian vision, the Baltic states might be tightened up by military means. The Vilnius Summit Communiqué specified, 'We cannot discount the possibility of an attack against Allies' sovereignty and territorial integrity' (Communiqué, 2023). Considering the current situation and NATO's Article 5 statement, the purpose of possible NATO forces' deployment in Latvia is to deter or prevent possible hostile activities from Russia or Belarus. Based on the mentioned above, Latvia must be capable of planning and implementing deterrence and defence operations on its territory while receiving NATO support.

This paper will argue that the level of development and technical condition of the Latvian land transport infrastructure meets NATO's division deployment requirements.

This paper aims to determine the readiness level of Latvian land transport infrastructure to ensure NATO's division deployment and preparation for further operations.

In the first chapter the author will define and describe deployment-supporting infrastructure and its military requirements. Next, the author will assume the incoming forces' size, task organization, and equipment. In the second and third chapters, the rail and road network will be analysed, as its condition, throughput capacity, and

determination of possible obstacles. In the fourth chapter, the author will outline requirements for staging areas and examine possible locations` suitability for military purposes. In the conclusion the author will consolidate key findings and provide organizational recommendations for national Graduated Response Plan development.

The author will use quantitative data collection and analysis methods to confirm the throughput capacity of road and rail networks and the dimensions and capacity of possible staging areas. The qualitative data collection and analysis methods will be used to determine the main problematic areas from the Subject Matter Expert (SME) perspective and design recommendations to develop land transport infrastructure from a military perspective.

The author will not utilize known NATO forces` units for the calculations. The imagined unit will be used to reflect the average size of the division (type/number of vehicles and space on the ground). The Rail Baltica project's end state and consequential advantages will not be determined because the project's completion term has not been defined yet. The author will review land transport infrastructure from the peacetime perspective and, consequently, will not consider wartime impact factors.

1. Deployment supporting infrastructure and deployable NATO forces` composition

In common understanding, the concept of logistics has been known since ancient times. Such objectives as the Chinese Grand Canal, the Roman Road network, and the Silk Road were serving for trade and movement of troops for centuries. For the first time in the Modern Era, the term “logistics” was used by the general of the Napoleonic army Antoine-Henri Jomini. General Jomini defined logistics as the ‘art of well-ordering the functioning of an army to assure its arrival at a named point’ (Komárek, 2019). A more accurate and comprehensive description of the military term ‘logistics’ is given in the US Field Manual 100-16: ‘Logistics is the process of planning and executing the movement and sustainment of operating forces in the execution of military strategy and operations’ (Kress, 2002).

Transportation is one of the logistics` functional areas. From the military perspective, the ability to transport personnel and materials effectively and efficiently within a transportation system is vital on operational and tactical levels. The European Commission confirmed this importance by issuing ‘The Action Plan on military mobility’.

Implementing the plan by the Member States implies developing and enhancing strategic transport infrastructure during 2021 – 2027 period and simplifying and standardizing rules and procedures by 2024 (mobility, 2019). The development of transport infrastructure will support the local trade market on the national and European level and enhance defence ability on NATO level.

Contemporary transport infrastructure is one of the most crucial components of logistics infrastructure. Transport infrastructure facilitates the development of connections between regions within a country and between countries, and consequently, it supports the formation of mutual economic, social, and cultural relations (Oksana Skorobogatova, Irina Kuzmina-Merlino, 2016). Land transport is an essential transport sub-group, encompassing road and rail (David Patrman, Alena Splichalova, David Rehak, Vendula Onderkova, 2019).

The military purposes of land transport infrastructure partially coincide with the state's objectives. Rapidity, efficiency, and convenience characterize not only trade's needs but also represent military logistics exigencies. From a military perspective, controlling, protecting, and maintaining land transport infrastructure is critical to ensure rapid and efficient deployment of forces. Control over the vital transport infrastructure nodes can have strategic implications during a crisis or conflict. In such a scenario, the Reception, Staging, Onward Movement (RSOM) process became one of the most essential activities that supports swift force buildup in the theatre. The RSOM supporting infrastructure consists of principal components: Aerial Ports of Debarkation (APOD), Sea Ports of Debarkation (SPOD), Marshalling areas, Holding areas, Staging areas, Assembly areas, road network, and rail network. Moreover, considering the Vilnius summit 2023 decision to exercise rapid reinforcement of any Alliance member regularly, 'demonstrating resolve and capability' (Communique, 2023), ensuring the ability to execute RSOM for incoming NATO divisional size unit is crucial. In this paper, the author will consider the land transport infrastructure: road and rail networks and Staging areas. In order to define the readiness level of Latvian land transport infrastructure, it has to be surveyed through the prism of a military point of view.

From a military perspective, land transport infrastructure needs to fulfil a number of particular requirements in order to serve the requirements of the armed forces. These requirements include strategic location, operational capacity, flexibility and adaptability, sustainability and resilience, and security. A strategic location ensures

that infrastructure objects are situated in areas easily accessible to land forces and interconnected with different transportation networks and communication systems. This enhances the usability of infrastructure and, optimizes transportation, storage and security resource utilization, and minimizes transportation distances. The most crucial advantage of a strategic location is saving time. Operational capacity is the maximum number of vehicles and materials an infrastructure component can maintain or pass through over a given period. It is essential to ensure that infrastructure meets the transportation and storage demands of land forces. The infrastructure needs to be sufficiently developed to provide a variety of options for operation planning. The ability to adopt alternative courses of action facilitates the execution of modified plans. For the land forces, it is essential to maintain flexibility and not stick to only one initial plan. Sustainability is paramount for infrastructure to ensure the long-term use and ability to be maintained at a certain level. Infrastructure must be strong enough to resist both natural disasters and man-made threats such as direct kinetic attack, bombing, and indirect fire. Security of transport infrastructure is one of the most critical requirements, and it consists of various methods, such as denial of unauthorized access, physical security, force protection, cover and concealment activities. To define the readiness level of Latvian land transport infrastructure, it has to be surveyed through the prism of a military point of view.

In order to estimate and calculate the expected load on Latvian land transport infrastructure, the author developed the artificial Divisional size unit (further in the text – the Division). Figure 1 represents the Division`s task organisation (TASKORG).

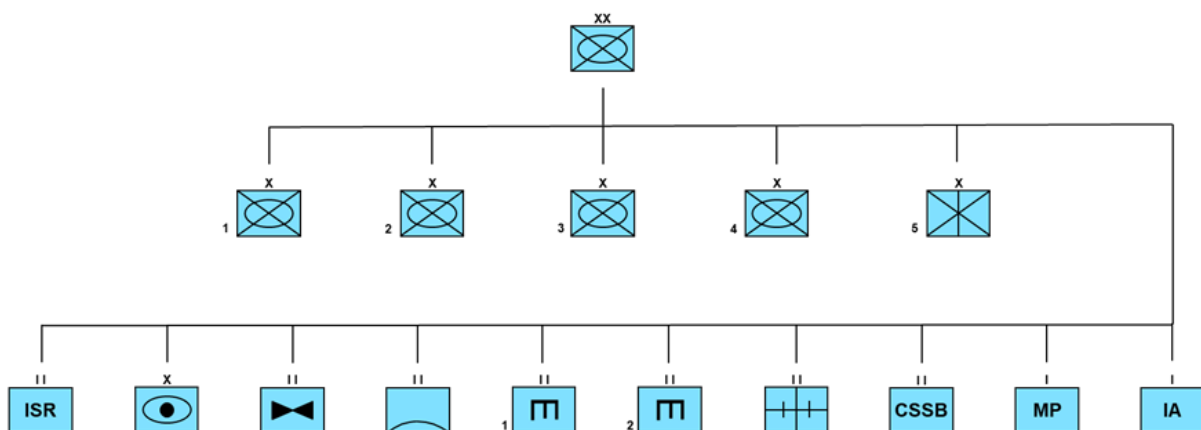


Figure 1. The Division`s TASKORG.
Source: Author`s own.

By creating TASKORG, the author leaned on the US doctrinal mechanized division and brigade layout and partially utilized the optimized structure of the Multinational Division North and the Latvian mechanized infantry and light brigades. As a result, the

artificially formed Division is comparable to the one that Latvia may host in the case of a war.

The Division consists of five manoeuvre brigades, one artillery brigade, one Intelligence Surveillance Reconnaissance (ISR) battalion, one Air defence (AD) battalion, two Combat engineer battalions, one Medical battalion, one Combat service support (CSS) battalion, one Military police (MP) company, and one Information activities (IA) company. For the computation purpose, the author has considered only the main combat, combat support, and combat service support platforms: tanks, infantry fighting vehicles (IFV), armoured personal carriers (APC), self-propelled howitzers (SPH), engineer tracked vehicles (ENG TKV), other tracked vehicles (other TKV), and logistical vehicles (LOG). For plausible calculations and reflection of the actual situation, the author has chosen one of the most popular platforms utilized by the Middle and North European armies (ArmedForces.eu). The AEV3 Kodiak has been chosen as an example for Combat engineer vehicle because it is an armoured engineering and mine clearance tank that can meet the technical and tactical needs of modern-day armed forces (army-technology.com). The MAN Type 464 LKW has been chosen as an average logistical truck in order to simplify calculations. This type of platform is widely spread across Europe's logistical units. The sizes and weights of the division's main platforms are combined in Table 1.

Vehicle type	Length (m)	Width (m)	Height (m)	Weight (t)	Platform used for table's data
TANK	9.97	3.75	3	55	Leopard 2 A5/6
IFV	6.55	3.1	2.7	30	CV-90
APC	7.88	2.99	2.37	25	Boxer
SPH	11.7	3.6	3.1	56	PzH 2000
ENG TKV	10.2	3.5	2.3	55	AEV3 Kodiak
OTHER TKV	4.8	2.7	2.5	13	M113
LOG	10.1	2.5	2.8	24	MAN Type 464 LKW

Table 1. Dimensions of the vehicle types.

Source:

Author's own.

The table shows that more than half of vehicle types are 30+ tons heavy, which provides two options to transport them: by heavy equipment transporters (HET) or by rail. A large amount of HET on the highways can cause traffic jams, road wear, and higher fuel consumption, which is logistical difficulty for transportation. To promote more efficient and sustainable transportation, rail transport offers a compelling

alternative. Rail transportation provides a persuasive option to encourage more efficient modes of transportation.

2. Rail network

Rail transport infrastructure in Latvia is developed and is widely used for civil cargo and passenger transport but is not widely used for military needs. The railway system has direct exit to Latvian sea ports, and this will support RSOM operation by strengthening multimodal transportation. Figure 2 shows that the railway infrastructure in Latvia connects the whole country. Railway lines connect the biggest towns and manufacturing centres of all districts.



Figure 2. Transport infrastructure of Latvia.
Source: (Transport).

Latvian railway network is interconnected with Lithuania in four crossing points and in two crossing points with Estonia, which provides an opportunity to execute cargo transportation to/from two NATO neighbouring countries.

The most essential interconnecting railway lines are in the mid-south of Latvia and the east-south of Latvia. Those railway lines allow the cargo delivery to the two biggest cities in Latvia: Riga and Daugavpils. According to the author's assumption, in the war case scenario, Daugavpils will not play any significant role in cross-border logistics because it is located just 33 km from Belarus and there is a cut-off threat. The author assumes that the Riga district will be used for the force accumulation process. The

assumption is based on the geographical location of the states' border with Russia and Belarus and the most likely adversary's avenues of approach from the Latvian eastern border towards Riga along highways A3, A2 and A6. From operational perspective, there are three railway lines to transport heavy (tracked) vehicles to Riga district, those are: Ventspils SPOD – Tukums – Riga, Liepaja SPOD – Jelgava – Riga and Kaunas (Lithuania) – Jelgava – Riga.

To calculate the railway line's throughput capacity, the author will use official data from Latvian Railways (Railway) and by author's created formulas. The maximum permissible train speed in the Latvian Railways infrastructure is set up to 90 km/h for freight trains. The author will use the platform type of wagon (platforms) for further calculations because the platform is used for the transportation of machinery, equipment, long cargo, and containers, which do not require protection from the weather (Bident).

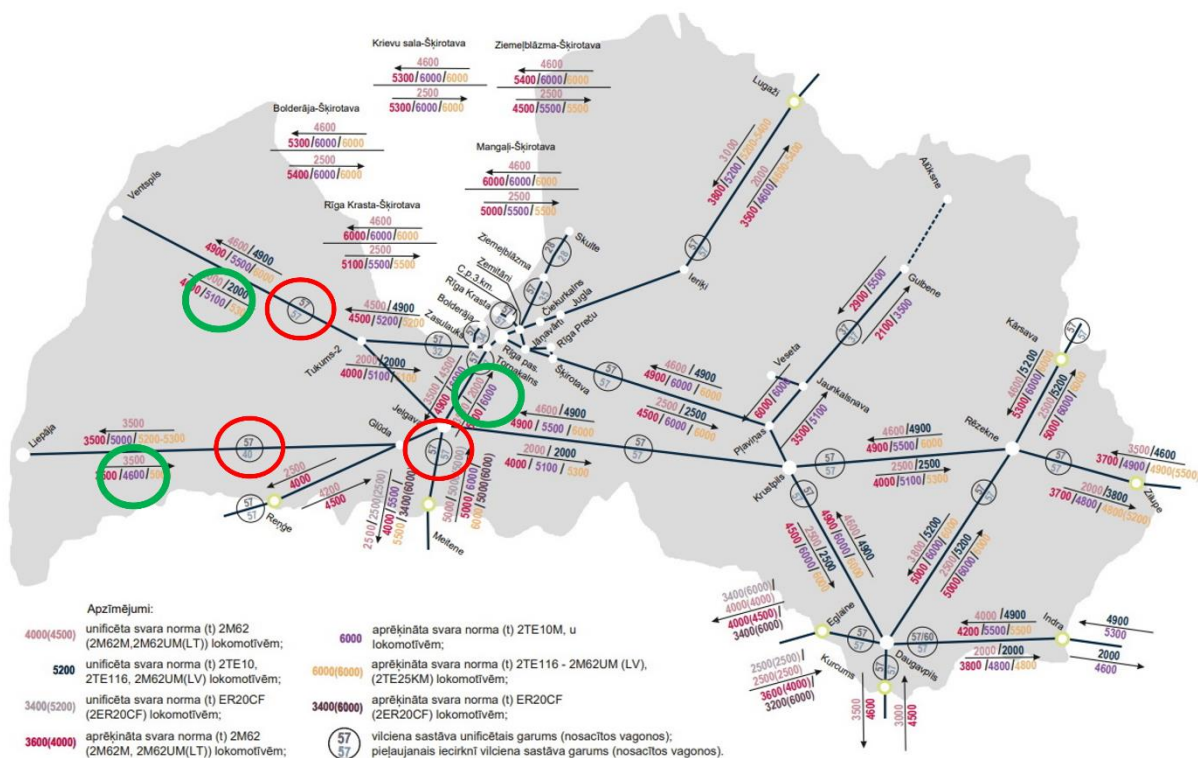


Figure 3. Norms of weight and length of freight trains based on Latvian Railway (Railways, 2021). Figure created by the author.

Figure 3 shows preconditions for calculation for three previously mentioned operational routes. The most important data is encircled by red (the length of the trainset in conditional wagons) and green (calculated weight norm for 2TE10M locomotives) rounds. The 2TE10M locomotives are the most towing capable in Latvian Railways. Taking into consideration the fact, that the unified length of the trainset in Latvian railway lines is 57 conditional wagons, the author has calculated how many platform

wagons it is possible to include in the composition of one train according to the formula:

$$N_{\text{wagon max.}} = \frac{N_{\text{conditional wagon max.}}}{l_{\text{conditional wagon's length}}} = \frac{57}{1.4} = 40 \text{ platforms.}$$

The factor 1.4 was used in the

formula based on Latvian Railways data – the platform wagon type's conditional length is 1.4. Next, the author has calculated the maximum weight of a freight train consisting of 40 platforms: $M_{\text{max train weight}} = 40 \text{ platforms} \times (26.5 \text{ t (platform's weight)} + 67.5 \text{ t (max. cargo weight)}) = 3,760 \text{ t}$. It may be concluded, that 40 platforms fit the weight limit of Latvian railways infrastructure, which is 6,000 t.

For operational purposes, as well as to reduce commute time, the author used both Ventspils and Liepaja SPODs. To calculate the time spent on a single trainset on the routes Ventspils SPOD – Riga, Liepaja SPOD – Riga, and Latvian border – Riga, the author has multiplied the real passenger train time with factor 1.5. Factor 1.5 is the author's assumption based on the maximum speed allowed, speed limits on different stages, locomotives' traction performance, and common cargo weight. The result of the necessary time for routes is: 7 h for Ventspils SPOD – Riga route, 5.6 h for Liepaja SPOD – Riga route, and 2.8 h for Latvian border – Riga route. To calculate throughput capacity, the author decided to simulate the transportation of the Division's heavy-tracked vehicles (tanks, SPHs, ENG TKVs) by railway. The total transportation time is tabulated in Table 2.

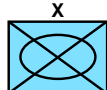
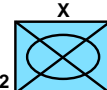
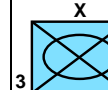
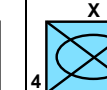
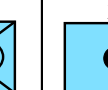
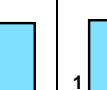
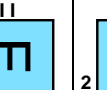
							
	1	2	3	4	1	1	2
	Number of vehicles transported by railway						
	136	120	120	34	42	31	31
Required number of trains	3.4	3	3	1	1	1	1
Route	Ventspils - Riga	Liepaja - Riga	Liepaja - Riga	Ventspils - Riga	Ventspils - Riga	Liepaja - Riga	Ventspils - Riga
Transportation time (h)	28	16.8	16.8	7	7	5.6	7
Unloading time (h)	12.6	11.1	11.1	3.7	3.7	3.7	3.7
TOTAL	5.8 days (137.8 h)						

Table 2. Estimated transportation time for combat and combat support platforms from SPODs Liepaja and Ventspils to the Garkalne railway station.
Source: Author's own.

To calculate the unloading time at the Garkalne railway station, the author has started by calculating the total drive-off distance and time for all vehicles on one freight train.

The limit of platforms for simultaneous unloading in Garkalne is 13 platforms (the length of the unloading railway line is 250 m). Using the formula: $S_{\text{common.distance}} = \frac{n(n-1) \times l}{2} = 1,037 \text{ m}$, where n is the number of vehicles, l is the length of the platform, the author has acquired a total drive-off time of 30 minutes at a speed of 2 km/h. The freight train shunting operation takes an additional 20 minutes (1 km with a speed of 6 km/h). Removing fasteners for 13 vehicles takes at least 30 minutes, when several drivers are available on the spot. The total unloading time for one freight train is three hours and 40 minutes (three unloading and two shunting operations).

From a military perspective, the significant issue of Latvian railway infrastructure is an insufficient number of ramps for loading and unloading vehicles. Moreover, there is only one ramp suitable for heavy-tracked vehicles in the Riga district – the Garkalne railway station, which is advantageous for the force deployment to the Riga district and North of river Daugava. In Latvian SPODs Riga, Ventspils, and Liepaja, there are no ramps for loading/unloading. Therefore, three options may be utilized. The first option is to use a local railway crane; however, this requires consideration of the crane's design features. The second option is to use a military wheel crane, but the loading and fastening of one cargo unit will take a minimum of 30 min. The third option is to purchase and utilize the mobile heavy-duty loading ramps.

The use of rail transport brings many advantages, such as significant carrying capacity and variety of cargo, however the transportation by road offers manoeuvrability, flexibility, and geographically precise delivery.

3. Road network

The European Commission's statement in 2018 was that 'Ratings for Latvia's transport infrastructure are close to the EU average, except for its roads, which are rated poorly.' (Commission). According to the Latvian State Roads corporation, Latvia has a relatively dense road and street network with a total length of 70,645 km, including 15,537 km with bituminous pavement, 53,606 km with crushed stone and gravel pavement, and 1,502 km of roads with no pavement (Roads, 2021). The road network connects all the state's towns, villages, and farmsteads. The total number of main roads connecting all Latvian regions is 15. Although the statistics show that only 22% of the Latvian road network is bituminous roads, this factor does not restrict cargo transit traffic. An important fact is that Latvia does not have high-speed highways with

a year-round speed limit of 110+ km/h. The technical condition of bituminous pavements on assessed roads is valued at the following percentages: very good – 25.6%, good – 25.1%, satisfactory – 18.6%, poor – 15.1%, very poor – 15.6%. The technical condition of gravel pavements on assessed roads is valued at the following percentages: good – 6.7%, satisfactory – 37.4%, poor – 55.9% (Roads, 2021).

From the military perspective, the presence of a developed road network is more important than the quality of the surface. An extended road network allows the designation of Main supply routes (MSR) and Alternative supply routes (ASR) on different levels: division, brigade, and battalion. Figure 4 represents the author's tactical analysis of the road network based on the terrain analysis and the previously mentioned adversary's probable avenues of approach. The main 15 roads are marked with red and yellow colours. The possible Assembly area (AA) for NATO's deployed forces is marked with a green oval. Blue arrows denote NATO forces transfer corridors with poorly developed road networks, which reduces the possibility of designating ASRs. According to the Latvian State Roads corporation, the most loaded by traffic intensity on the main state roads in recent years are Riga bypass roads A4 and A5, as well as connecting Latvia and Lithuania roads A7 and A8 (Roads, 2021).

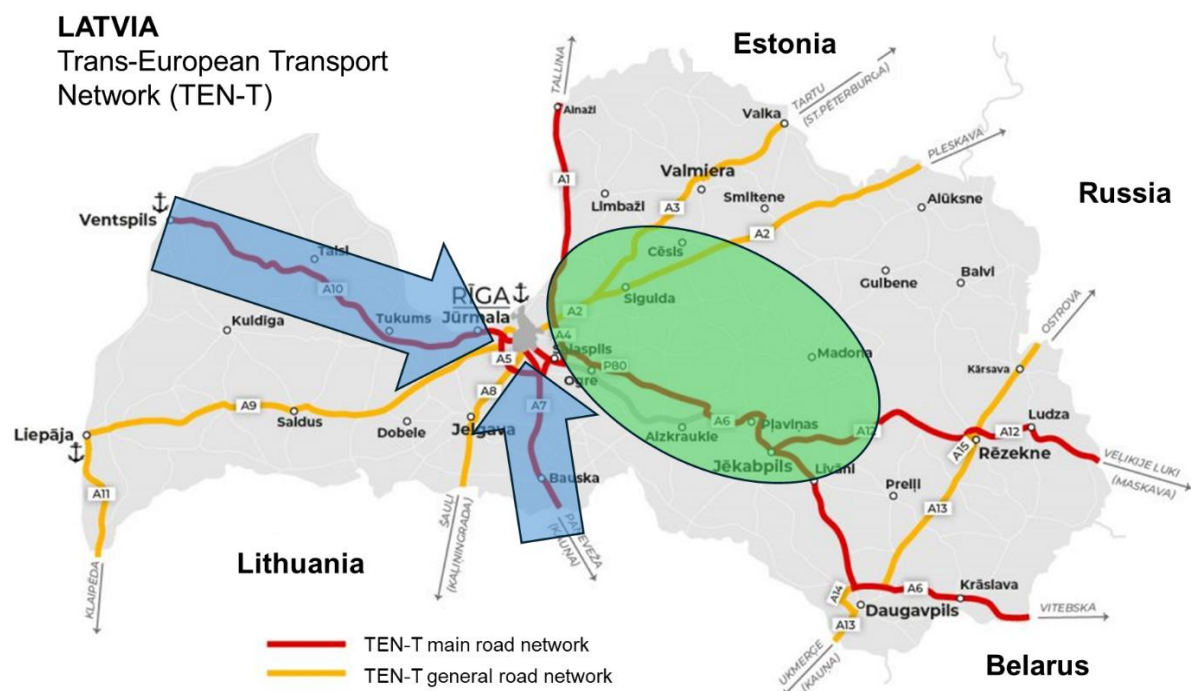


Figure 4. Tactical analysis of the road network based on Berzina (2021). Figure created by the author.

To calculate roads' throughput capacity, the author decided to simulate the transportation of the Division's IFVs and other TKVs by HETs and simulate the

movement of the Division`s APCs and LOG vehicles in convoys. The author`s model assumes multimodal transportation of some units with the cross-loading in Latvian SPODs and the arrival of some units by ground, crossing the Lithuanian border. All previously mentioned vehicles are proportionally divided into four routes to distribute traffic load and to save total deployment time. The author has chosen the Lithuanian border crossings on Latvian main roads A8 and A7 and SPODs Ventspils and Liepaja as the route starting points. For the Release point (RP), the author has chosen the village of Tinuzi, which is slightly shifted to the southwest centre of Divisional AA. Figure 5 represents all four routes crossing or bypassing Riga city. The total deployment time for the Division`s IFVs, APCs, other TKVs, and LOG vehicles using the Latvian road network is tabulated in Table 3.

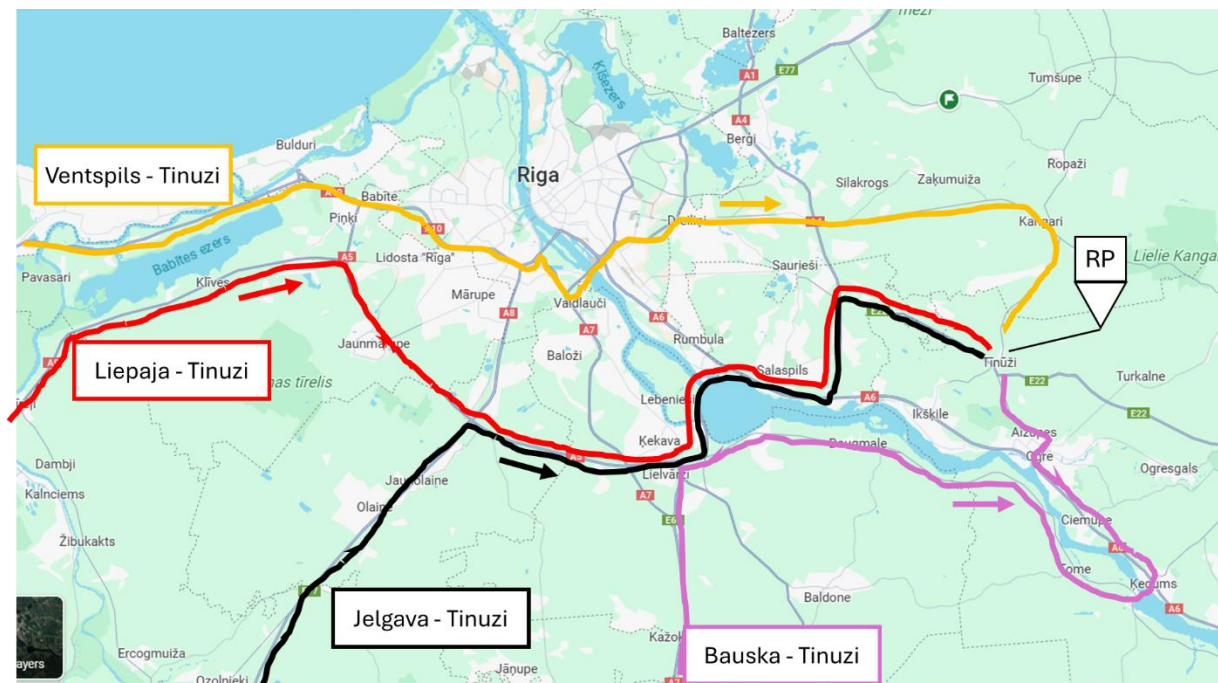


Figure 5. Convoys` routes crossing or bypassing Riga.

Source: Author`s own.

For deployment time calculations, the author used the following data:

- The average speed of the convoy is 60 km/h for each route.
- The convoy consists of 9 – 12 vehicles.
- The time gap between convoys is 3 minutes, and between every 10 convoys is 10 minutes.
- No short-stops planned.

The author's calculations do not consider civilian movement on designated routes and the ensuing consequences. In the actual situation, factor 2 can be used for the appropriate time calculations.

Route	Unit	Vehicles		Number of convoys within unit	Travel time of one convoy (60km/h)	Route congestion time
		type	number			
Ventspils - Tinuzi, 227 km	1.BDE	IFV	91	44	2 h 20 min.	6 h 10 min.
		other TKV	31			
		LOG	318			
	1.ENG BN	IFV	18	8		
		other TKV	3			
		LOG	65			
	ARTY BDE	other TKV	16	7		
		LOG	52			
	ISR COY	IFV	12	2		
		LOG	8			
Liepaja - Tinuzi, 254 km	2.BDE	IFV	106	47	2 h 30 min.	6 h 23 min.
		other TKV	30			
		LOG	332			
	2.ENG BN	IFV	18	8		
		other TKV	3			
		LOG	65			
	MED BN	APC	16	4		
		LOG	30			
	AD BN	IFV	12	3		
		other TKV	2			
		LOG	20			
LTU - Jelgava - Tinuzi, 104 km	4.BDE	IFV	123	37	1 h	4 h 53 min.
		APC	86			
		other TKV	4			
		LOG	160			
	5.BDE	APC	40	25		
		other TKV	4			
		LOG	205			
LTU - Bauska - Tinuzi, 118 km	3.BDE	IFV	106	47	1 h 11 min.	4 h 49 min.
		other TKV	30			
		LOG	332			
	CSS BN	other TKV	7	10		
		LOG	90			
	MP COY	LOG	4			
	IA COY	LOG	4			

Table 3. Estimated routes' congestion time during the forces' deployment to the Assembly area near the village of Tinuzi.

Source: Author's own.

Table 3 shows the sufficient throughput capacity of designated routes for NATO force transfer to the AA. There should be no perceptible issues if careful planning and preparation are done. Calculating the required quantity of HETs for IFVs and other TKVs transportation, the author considers that foreign companies' HETs will be utilized

for transferring vehicles from the southern direction. At the same time, the number of to-be-transported vehicles from Ventspils and Liepaja is 171 each. Contracting 342 HETs simultaneously is doable in Latvia. The author does not have information how many HETs belongs to Latvian Transport Companies, but according to the Official statistics of Latvia the total number of freight carriers in Latvia is 92,500 (Bureau, 2021). Based on data provided by Latvian Mechanised Infantry Brigade G-4 branch head, Latvian Transport Companies possess approximately 50 HETs with semi-trailer platforms with a lifting capacity of 60 t and 5,000 – 6,000 HETs with semi-trailer platforms with a lifting capacity of 25-30 t. The author assumes 2,000 HETs are used in Latvia.

4. Staging areas

The RSOM process is an inherent element of the force buildup in the theatre, and the passage of incoming forces through a staging area is an intrinsic element of RSOM. The staging area (SA) is used for assembling and organizing the unit, final maintenance, and uploading of the basic loads and supplies (Wade, 2018). Generally, personnel and unit equipment meet in the staging area. SA must meet specific requirements to ensure continuous preparation and scheduling of further movement to the tactical assembly area. Those requirements are proximity to the MSR, sufficient area and hard ground, power and water supply, short time accommodation for troops, preferably cover and concealment.

For the calculation of the minimum required SA, the author assumed the following condition: there must be a two-meter radius around the dimension of the vehicle. Then, following the previous division of the vehicles by transportation mode (by road or railroad), the author counted and summarized the data in Figure 6. According to the author's calculations, the total minimum area for tracked vehicles is 30,970.32 square meters or 0.03 square kilometres, and the total minimum area for wheeled vehicles is 141,665.76 square meters or 0.14 square kilometres. To analyse SA's possible locations, the author considered all specific requirements as well as general location – north of river Daugava and proximity of the release points for the railroad and road routes.

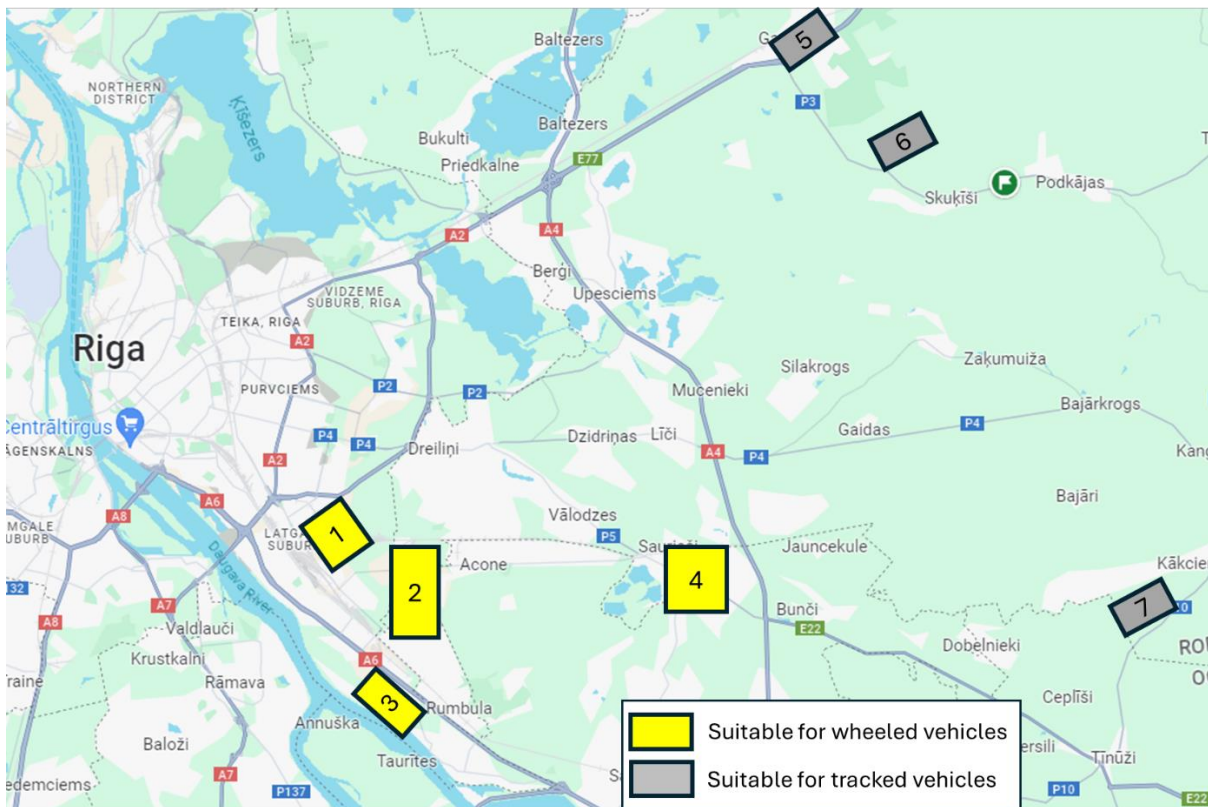


Figure 6. Possible staging areas near Riga, north of the river Daugava.

Source: Author's own.

Figure 6 represents locations appropriate for SAs in vicinity of Riga. The author has identified four SAs for wheeled vehicles with a total area of 8.22 square kilometres and three SAs for tracked vehicles with a total area of 3.8 square kilometres. The total area of potential staging areas significantly exceeds the minimum required areas. SA1 is located between the A2 and A6 main roads in an industry territory. SA1 has a developed bituminous road network and provides a considerable number of warehouses and hangars, as well as electricity and water supply. SA2 is located 3 km north of the A2 main road in an industry territory. SA2 has a mostly bituminous road network and provides several warehouses and hangars. SA2 ensures a truck workshop and electricity and water supply. There are eight open areas 250x100 m and separate groves in the southern part. SA3 is located in the south next to the A2 main road in the territory of the former airfield. SA3 has several hangars and a truck workshop, providing electricity and water supply. There are concrete squares 250x80 m in the middle and a concrete runway and open areas along the south side. SA4 is located 1.5 km west of the A4 main road in a partially industry territory. SA4 has a moderate bituminous road network and several hangars, providing electricity and water supply. There are several concrete squares mixed together with groves. SA5 is located next to the Garkalne rail station in a partially industry territory. SA5 mainly has a gravel road network and several hangars, providing electricity and water supply. The eastern

part provides noticeable concealment opportunity. SA6 is located 4 km south of the A2 main road and 5 km from the Garkalne rail station in a coniferous forest. SA6 has a few open areas and cops woods. SA7 is located 14 km east of the A4 main road and 9 km north of the A6 main road in a coniferous forest. SA7 has several open areas and cops woods. Based on data provided by Latvian Logistics Command, as the Host Nation, Latvia can afford short-term accommodation for 10,000 troops simultaneously. In the SAs, Latvia is able to ensure necessary amenities, such as accommodation in air-conditioned tents, separate tents for dining rooms, mobile restrooms, and showers. The author considers the SA's capacity of 10,000 troops sufficient to conduct force build-up in the theatre because the transfer of divisional forces will be split by brigade and battalion-size units and will not be executed simultaneously. Almost all potential staging areas provide all necessary conditions for the unit's rapid and continuous assembling and organizing.

Conclusion

The development of land transport infrastructure is an essential investment in the State's security. By investing in it and thinking from a military perspective, a country can ensure that its armed forces are able to fulfil their missions effectively and protect the nation from harm. Summarizing the calculations results, environment description, and theoretical basis, the author made the following conclusions.

First, the deployment supporting infrastructure in Latvia is constantly evolving to meet the European Commission and NATO requirements. Latvian National Defence Forces have a wealth of expertise utilizing the land transport infrastructure while conducting tactical level exercises and assisting the Allied forces during peacetime.

Second, the railway network generally supports RSOM, however there are some issues to consider. The Riga rail station is the chock point to reach the area of operation north of river Daugava. The railway infrastructure owns insufficient number of ramps for loading and unloading vehicles. The railway lines have a reasonable throughput capacity, regardless of the carriage of civilian cargo. Nonetheless, the simultaneous transportation of civilian cargo throughout the RSOM may turn into a major challenge.

Third, the road network is mid-level developed and supports RSOM. However, two of the four NATO forces` transfer corridors towards Riga have poorly developed road

networks. Bridges over the river Daugava near Riga create a choke point for transportation.

Fourth, Latvia has sufficient dispersed territories suitable for staging areas' purposes.

Recommendations

Several recommendations should be considered in order to sustain and improve Latvian land transport infrastructure to support NATO division-size forces' deployment in Latvia.

First, obtaining the heavy-duty mobile railroad ramps would provide a more flexible strategy for selecting the final destinations and expedite the transfer of forces.

Second, defining priorities and developing a movement plan would deconflict civilian and military cargo transportation from SPODs toward the centre and east of Latvia.

Third, developing a detailed movement plan would prevent bottleneck effects in the vicinity of bridges over the river Daugava and deconflict the usage of roads between incoming military forces and the flow of displaced persons.

Fourth, developing a comprehensive, timely, and accurate plan for establishing and leaving staging areas would contribute to expediting the force build-up process.

Finally, organization of international military exercises with sufficient use of land transport infrastructure would contribute identifying and eliminating infrastructure weaknesses.

Bibliography

2017. Allied Joint Movement and Transportation Doctrine (AJP-4.4). *AJP-4.4*. 2017.

ArmedForces.eu. ArmedForces.eu . *ArmedForces.eu* . [Online] ArmedForces.eu . [Cited: 16 November 2023.] https://armedforces.eu/land_forces/tanks.

army-technology.com. army-technology.com. *www.army-technology.com*. [Online] [www.army-technology.com](https://www.army-technology.com/projects/kodiak-vehicle/). [Cited: 16 November 2023.] <https://www.army-technology.com/projects/kodiak-vehicle/>.

Bident. Bident Global Logistics official Web Page. *Types of railway wagons*. [Online] Bident Global Logistics. [Cited: 15 November 2023.] <https://bidentlogistics.com/railway-wagons-types-and-sizes/>.

Bureau, Central Statistical. 2021. Central Statistical Bureau of Latvia official Web Page. *Transport in Latvia 2021*. [Online] 2021. [Cited: 7 December 2023.] https://admin.stat.gov.lv/system/files/publication/2021-08/Nr_17_Transports_Latvija_2021_%2821_00%29_LV_EN.pdf.

Commission, European. European Commission official Web Page. *EU Transport Scoreboard*. [Online] [Cited: 20 November 2023.] https://transport.ec.europa.eu/system/files/2018-03/lv_en.pdf.

Communique, Vilnius Summit. 2023. NATO official Web Page. *Vilnius Summit Communique*. [Online] 19 July 2023. [Cited: 01 November 2023.] https://www.nato.int/cps/en/natohq/official_texts_217320.htm.

David Patrman, Alena Splichalova, David Rehak, Vendula Onderkova. 2019. *Factors Influencing the Performance of Critical Land* . Novy Smokovec : 13th International Scientific Conference on Sustainable, Modern and Safe Transport , 2019.

Edwards, John E. 2000. *Combar Service Support Guide*. Mechanicsburg : Stackpole Books, 2000.

Evans, Carol V. 2022. *Enabling NATO's Collective Defense: Critical Infrastructure Security and Resiliency*. Carlisle : US Army War College, 2022.

Fiott, Daniel. 2017. European Union Institute for Security Studies official Web Page. *www.iss.europa.eu*. [Online] November 2017. [Cited: 04 October 2023.] <https://www.iss.europa.eu/sites/default/files/EUISSFiles/Brief%2031%20Military%20mobility.pdf>.

Heinrich Brauss, Ben Hodges and Julian Lindley-French. 2021. Center for European Policy Analysis Official Web Page. *www.cepa.org*. [Online] 03 March 2021. [Cited: 04 October 2023.] <https://cepa.org/comprehensive-reports/the-cepa-military-mobility-project/>.

Henderson, James H. 2008. *Military Logistics Made Easy*. Bloomington : AuthorHouse, 2008.

Komárek, Jaroslav. 2019. *The roots of military logistics in a retrospective.* Brno : the University of Defence, 2019.

Kress, Moshe. 2002. *Operational Logistics. The Art and Science of Sustaining Military Operations.* . Boston : Center for Military Analyses, Israel, 2002.

mobility, Military. 2019. European Parliament official Web Page. *Military mobility.* [Online] 2019. [Cited: 03 November 2023.] [https://www.europarl.europa.eu/RegData/etudes/ATAG/2019/635570/EPRS_ATA\(2019\)635570_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/ATAG/2019/635570/EPRS_ATA(2019)635570_EN.pdf).

Oksana Skorobogatova, Irina Kuzmina-Merlino. 2016. *Transport Infrastructure Development Performance.* Riga : 16th Conference on Reliability and Statistics in Transportation and Communication, 2016.

Railway, Latvian. Latvian Railway Cargo. *ldzcargo.ldz.lv.* [Online] [Cited: 15 November 2023.] <https://ldzcargo.ldz.lv/en>.

Railways, Latvian. 2021. Latvian Railways official Web Page. *Norms of weight and length of freight trains based on Latvian Railway.* [Online] 2021. [Cited: 7 November 2023.] <https://www.ldz.lv/lv/tikla-parskats-2023>.

Roads, Latvian State. 2021. Latvian State Roads official Web Page. *State Road Network Statistics 2020.* [Online] 2021. [Cited: 5 December 2023.] <https://lvceli.lv/wp-content/uploads/2021/07/LVC-Statistika-2020-20210729-1335.pdf>.

Smith, Jeremy C D. 2018. *Defence Logistics.* London : Kogan Page Limited, 2018.

Transport, Ministry of. Ministry of Transport Republic of Latvia. *www.sam.gov.lv.* [Online] Ministry of Transport Republic of Latvia. [Cited: October 10, 2023.] <https://www.sam.gov.lv/lv/transporta-logistika>.

Wade, Norman M. 2018. *The Sustainment & Multifunctional Logistics Smartbook.* Lakeland : The Lightning Press, 2018.

VIKTORAS BUIVA. The Fourth Imperialistic Wave Inside of Russia and Options for Sustainment.

Introduction

With the fall of the Berlin Wall in 1989 and the following collapse of the Soviet Union (SU) in 1991, the liberal and democratic world order suggested the end of ideological conflicts. The promise of peace and stability worldwide and the absence of East-West tensions were expected. Although the collapse of the SU signified the end of Russia's imperial era, the leaders who followed still bore the mindset of imperial Russia. The notions about Russia's global dominance, its cultural superiority, and the need to restore the lost territories look out of place in today's post-imperial world (Mankoff, 2022).

This research will centre on Russia's imperialistic ambitions and the current implications of such behaviour. To understand how Russia is altering the liberal democratic order, we need to understand Russia's imperial political practices and imperial legacy. It is important to comprehensively understand Russia's present geopolitical position and its complex interactions with neighbouring countries. Therefore, it is crucial to comprehend the historical backdrop of Russia's imperialistic endeavours. This will support the arguments presented later in the research paper. Imperialism refers to a state's policy, practice, or promotion of expanding its power and authority regardless of rules-based international order. Russia's imperialism is achieved by acquiring territories or establishing political and economic dominance over other regions that Russia thinks are lost because of the collapse of the Russian Empire and the SU. Russia's imperialism violates the political autonomy and sovereignty of individuals (Sanborn, 2014).

Starting in the 16th century, Russian imperialism marked the historical policies and practices of territorial expansion pursued by the Russian Empire. As defined in political science today, evidence of imperialism was already found in the time of the Moscow Tsarist Empire. During that period, the Russian authorities gave priority to geographical expansion rather than the unification of the nation (Mankoff, 2022). We can outline at least three evolutionary stages of the Russian empire.

First, Russia under Ivan III, Vasiliy III, and Tsar Ivan the Terrible, so named "Tsar Russia", when Russian foreign and domestic policy exclusively concentrated on the ruler's and the empire's interests. Russia's territorial expansionism towards the east and south, military conquests, strategic partnerships, and interest in acquiring warm-water ports and controlling crucial trade lines provided a favourable basis for its imperialistic goals (Cohen, 1996).

Second, the Russian Empire under the Romanov dynasty. In particular, the expansion of Russia's physical boundaries and geopolitical power was encouraged by the significant contributions of Peter the Great and Catherine the Great. Russia's land acquisition along the Baltic Sea established vital access to important trade routes and warm-water ports. Further expansion into Eastern Europe, including Belarus, Ukraine, the Kingdom of Poland, and the Grand Duchy of Lithuania, strengthened Russia's supremacy in the region (Cohen, 1996). Moreover, Russia's expansion into the Caucasus and Crimea solidified its dominance in the Black Sea region and secured the main trade routes. Additionally, Peter the Great intended to modernise and adopt Western practices. This, in turn, contributed to strengthening Russia's imperial ambitions (Cohen, 1996).

Third, the imperialistic idea continued into the 20th century with the establishment of the Soviet Empire. Although it did not convey the conventional definition of an empire like previous Russian empires, it might be considered as the final embodiment of Russian imperial authority in a broad sense (Cohen, 1996). The concept of **Russia's imperialistic ambitions has been a repetitive leitmotif throughout its history. Therefore, we can expect a fourth wave of imperialism in the future.** Are we victims of efforts and attempts to create the fourth wave of the Russian Empire—the "Putin Empire"? This is one of the questions that will be answered in this research.

Nowadays, Russia is a broad imperial historical continuer that originated with the mediaeval Tsardom of Russia. This empire aims to replicate its ideology and political structure in various geographical areas. New forms of imperialism replaced it over time. They easily incorporate past knowledge and adapt to current demands and challenges. It attempts to establish proper systems to handle the affiliation between the central power and its periphery in imperial territories (Zaporozhchenko, 2023). This paper will

demonstrate the contemporary manifestation of Russian imperialism by examining its pursuit of creating a Pan-Slavic union (transformed and referred to as the "Russian world" today) in the post-Soviet region. Additionally, the research paper will explore the challenges faced by Russia in maintaining its imperial power and its attempts to re-establish the SU. This analysis will focus on the imperial realm and Russia's ability to sustain it.

This paper aims to prove that Russia does not have the political means to sustain its imperialistic ambitions because of a limited social-political influence, a weak economy, and insufficient military power. To achieve this aim, an analysis of the mentioned capacities will be conducted by examining the case of so-called Pan-Slavic Union imperialism and Putin's attempts to re-establish the SU as the most recent Russian empire example.

The research paper will discuss Russia's ability to sustain imperialistic ambitions, influence in core Slavic nations, and position as a protector of Slavic interests. Thus, the hypothesis of this paper is that Russia has no military, economic, social, or other resources to sustain its imperialistic ambitions over Ukraine or Belarus. First, the analysis will outline the social-political aspects and ambitions to impose the Pan Slavism idea in the two abovementioned core Slavic nations. The analysis will show the relationship between Pan-Slavism, considering its historical context and present-day expressions in its ties with Belarus and Ukraine. The second part will analyse the Russian fourth wave of imperialism and Putin's attempts to re-establish the SU from an economic and military perspective. Finally, based on the analysis, this paper will provide conclusions and potential projections regarding Russia's regional power. By examining these factors' complex interplay, we will understand whether Russia has the proper political means to sustain its imperialistic ambitions.

1. The Imposition of the Pan-Slavic Union over Belarus and Ukraine

The country, projecting itself as an empire, takes roots in imperialism from a historical background and socio-political aspects. Russia considers itself a key element of the Russian world's civilisational community (RF FA Ministry, 2023). Throughout history, the Pan-Slavism idea has been used as a social-political tool to further Russia's imperialistic ambitions and justify its expansionist policies. Further analysis will answer

the question of what precisely the Pan-Slavic idea is, what its transformations are, and whether it remains a powerful force in Russian foreign policy nowadays. Two core Slavic countries were taken for this analysis.

According to Suslov, Čejka, & Đorđević (2023), Pan-Slavism is not a clear and organised ideology but rather an assortment of political concepts, policies, and geopolitical aspirations. According to this ideology, all individuals who share Slavic legacy, culture, and language should have cultural and political cohesion among themselves – a “pan-national” identity.

Initially, Pan-Slavism's objective was to unify all Slavic people under one political and cultural system in the 18th century. The primary idea was to resist the domination of non-Slavic powers, such as the Ottoman Empire, the Habsburg Empire, and the Austro-Hungarian Empire. However, Pan-Slavism later transferred into a political and nationalistic idea that supported Russian autocracy and the Orthodox faith (Boeckh, 2016).

Modern Russian Pan-Slavists were inspired by two primary sources: the historical alliance of former socialist nations united by their ideological opposition to the West and the shared ethnocultural characteristics of the Slavic countries (Đorđević, et al., 2023). However, the question still exists of whether Russia, as a portrayed central Slavic state, can influence at least core Slavic countries' internal social-political processes at the level at which the empire should impact the subordinate states.

The collapse of the SU in 1991 pushed back Russia as the centric Slavic country able to keep power in the post-Soviet core countries such as Ukraine and Belarus. This weakened Russia's ability to project its influence in the region, making it more difficult for Russia to project the Pan-Slavic Union idea and support pro-Russian governments or movements.

This aspect is essential for Russia to live up to its imperial ambitions. Belarus, for example, officially supports Pan-Slavic ideas, initiatives, and narratives today. Nevertheless, the understanding of Pan-Slavism is narrower and basically about the unity of the three East Slavic peoples: the Russians, the Ukrainians, and the Belarusians. Additionally, despite the positive attitude of Lukashenka towards Pan-

Slavic ideas, the use of those ideas is no more than a tool used for the president's regime's political manoeuvrings (Suslov, et al., 2023).

Belarusian nationalism has consistently rejected the classical manifestation of Pan-Slavism. Furthermore, before 1918, one of its primary political objectives was reinstating the Grand Duchy of Lithuania in collaboration with the Lithuanians. Pan-Slavism had no relevance to this aim. Changes occurred during Stalin's rule. Cultural and political leaders of the BSSR were eradicated, educational materials were prohibited, and the previous imperial notion of the Great Russian people resurfaced and persisted for an extended period (Suslov, et al., 2023). Despite that, today we see a strengthening movement (Litvinism) which sees Belarusians as the former leading actor of the Grand Duchy of Lithuania and emphasises the ethnical dependence on the Baltic group.

Analysing the representative statistics, we see that the behaviour of the Belarusian President reflects society's opinion. Even though pro-Russian sentiments are typically predominant in the nation, just over a third of Belarusians agree with them. Approximately an equivalent number of individuals tend to favour a neutral stance on foreign policy. The fact that Belarusians show a prevalence of support for neutrality in international relations indicates a significant level of distancing from Pan-Slavic ideas. Despite declarative Pan-Slavic ideas by the President and its structures of power, less than half of Belarusians support integration with Russia. Moreover, even proponents of Pan-Slavism maintain a certain level of separation from Russia when it comes to their viewpoints on facets of integration (Bikanau, et al., 2023).

Lukashenka, to keep its regime alive, is forced to strike a balance between the fictitious history of a great country used to include the Great Duchy of Lithuania and the Soviet legacy as a basis for the creation of contemporary Belarus (Policy Meeting on the Implementation of Historical, 2022). To sum up, pro-Russian and pro-Pan-Slavic sentiments among Belarusians are more declarative than reflecting real will and efforts to reunite with Russia or create one pan-Slavic nation.

Another core Slavic country demonstrates a strong distancing from Russia and its Pan-Slavic union concept. Pan-Slavic ideas influenced Ukraine and Belarus in the 19th and 20th centuries, particularly during the SU period. Nevertheless, right after the collapse

of the SU, Ukraine employed balancing between Russia and the West. At the beginning of the 21st century, up to two-thirds of Ukrainians wished to be part of the EU and any form of post-SU organisation led by Russia. Firstly, heavily Russified Ukrainian cities demonstrated a pro-East stance. Secondly, the Orthodox Christian creed provided essential support for the Pan-Slavic idea. However, by 2012, according to the statistics, pro-Western supporters took over against those who supported Eastern integration, which stimulated the Maidan event in late 2013 and early 2014 (Suslov, et al., 2023).

Ukrainian Slavophiles, one of the most traditional Pan-Slavic union supporters, adopted Western ideas about democracy, constitutionalism, and federalism, claiming they were inherent to Ukraine's traditions. This laid the foundation for modern Ukrainian nationalism (Suslov, et al., 2023). They no longer needed Pan-Slavic ideas, mainly after Russia used them to justify its imperial expansion. This shift in opinion (see Table 1) shows how drastically attitudes towards Russia were shifting after the occupation of

Table 1. Ukrainian's changing attitudes toward Russia, Russian Leadership, and the project of the Russian-led East Slavic Union, with 2014 as the turning point

What is your attitude toward the Russian Federation? (positive/negative, %)	nd	85/9	82/10	34/51	37/46
What is your attitude toward the president of the RF Vladimir Putin? (positive/negative, %)	nd	53/32	47/40	16/75	10/81
Would you like Ukraine to join the union with Russia and Belarus? (yes/no, %)	61/21	56/25	49/29	22/62	20/62

Crimea.

(Suslov, et al., 2023)

According to Suslov (2023), around 22% still declare Russian as their native language, while only 6% identify as ethnic Russians. Very illustrative distancing from Russia and any Pan-Slavic or Russian World idea we can see in the statistics of the most Russified regions (f.e., Odesa and Kharkiv), where in 2014, only 12% of respondents agreed with the statement that they belong to the Russian World. Other eastern regions, such as Kherson and Zaporizhzhia, prove even more significant distancing, where the same questioning numbers reach only 6%, Dnipro 3%, and Mykolaiv 0%.

To sum up, the classic idea of "Pan-Slavism" now seems like an outdated concept, a utopian ideology that belongs more to the pages of history books than to the modern

world. This impression is partly strengthened by the current political climate, where two of the most significant Slavic nations, Russia and Ukraine, are involved in the war triggered by the Russian invasion. Belarus, balancing its identity and alliance with Russia and between the West and the East in foreign policy, pursues more pragmatic goals and benefits for the regime. Furthermore, the older generation's attitudes toward SU impact the figures expressed in statistical data for Russia's support. Therefore, it is likely that, with the change of generations, Lukashenko, or any future dictator, will find it increasingly difficult to maintain a balance and rely on outdated Pan-Slavic ideas. Consequently, Pan-Slavism, which once inspired Slavic nations, appears to be defunct.

Russian propaganda has attempted to create the idea of a single Slavic culture and ethnicity. However, Slavic is nothing more than a language group. Russia's imperialistic ambitions force it to seek alternative, non-military methods to expand its power. In support of this argument, we can see the importance of non-military means in Gerasimov's doctrine. The document emphasises its future crucial role, priority in development, and weight comparable with conventional countries' capability development in a relationship of 7 to 3 in favour of "soft power" (Olszanecka, 2021).

Slavic identity alone is too limiting for Russia, a post-imperial nation with a diverse population and a growing Muslim minority. This makes any attempt to promote pan-Slavism seem artificial and instrumental. The changes in Russia's geopolitical culture and regime ideology have revitalised Pan-Slavism, forcing it to look for fresh connotations that effectively convey contemporary political concerns and ideas. Considering that the Putin regime has shown its ability to adapt its ideology to different audiences, using the Eurasianist, *Rossiyan*, or Russian World (*Ruskij Mir*) language units (Grikontas, 2018).

The concept of the Russian World focuses not on the state's affiliation with the Pan-Slavic Union but rather on an individual who can identify with the "artificial" world. This new socio-political strategy of Russian soft power has played a vital role in the discourse of Russian social policy in the post-Soviet region. Nevertheless, it is challenging to implement for several reasons. Firstly, creating a "Russian world" is not only the cultivation of language and culture but also the attribution of a person itself, which is challenging to achieve abroad. Post-Soviet countries have an adverse history

with Russia, dating back to SU times. The critical mass of those who speak Russian and keep Russian culture in the family position themselves as residents of their country or city and not part of the artificial "Russian world". Secondly, even though Putin paid particular attention to the idea of the Russian world (Olszanecka, 2021), the successful integration of national minorities in post-Soviet states shows Russia's limited ability to reach Russian-speaking people abroad. After the occupation of Crimea and the beginning of the Russia-Ukraine war, the alienation of Russian-speaking people from any ties with Russia is visible. Countries such as Poland and the Baltic states express their highly negative attitude towards Russia's actions and are steamrolling in support of Ukraine's support issues.

We cannot deny that the Russian propaganda machine still manages to reach a specific part of the post-Soviet Russian-speaking society. However, this is a relatively small segment of the population, and it does not provide the necessary conditions for Russia's efforts to redraw the borders of the SU from a social perspective. People who were a target audience for Pan-Slavic and "Russian World" ideas seem to be in a distancing identity transition from Russia. This will be more visible with the inevitable change of generations and values in post-Soviet countries.

2. Reestablishment of the Soviet Union.

The Russian fourth wave of imperialism and Putin's attempts to re-establish the SU will be analysed from an economic and military perspective. Do we see prerequisites Russia met to position itself as an Empire in the short- to medium-term future? Firstly, we must understand what indications we see for imperial territorial expansion. Secondly, what is the actual country's economic strength? Thirdly, existing military power will be analysed from quantitative and qualitative perspectives.

The collapse of the SU was undoubtedly one of the most painful events in Russian imperialist history. The SU played a significant role in affecting Russia's imperialistic behaviour and served as an inspiration to restore former glory. Since the first days of Putin's coming to power, the westernisation vector predicted after the collapse of the SU has changed. Steps were taken to restore the mental connection with the SU and restore the state's former imperial power: glorifying achievements, returning the

anthem of the SU, strengthening the vertical of power, and reducing the external influence (Dugin, 2017).

President of Russia Vladimir Putin employs aggressive foreign policy strategies that mirror his imperialistic ambitions. He sent the first signals in his 2007 Munich Security Conference speech. Putin showed a profound shift in Russia's foreign policy - a more forceful and confrontational approach towards the West. The speech revealed Russia's remaining imperial aspirations, willingness to regain influence, and lost status as a global superpower. Putin opposed NATO expansion out of fear that Russia may lose the territories he believed belonged to it (Putin's famous Munich Speech, 2007).

Russia's imperial legacy and ambitions permeated the speech, laying the groundwork for the subsequent conflicts in Georgia (2008), the annexation of Crimea (2014), and the ongoing war in Ukraine. Here we may observe the repercussions of Russia's "Empire nostalgia", efforts, and attempts to create the fourth wave of the Russian Empire - the "Putin Empire".

Russia aims to recover territorial and power losses that resulted from the collapse of the SU by annexing the territories of neighbouring states. Mankoff (2022) views Putin's invasion of Ukraine as a manifestation of the Russian elite's ambition to re-establish an imperial Russia. Putin aims to rebuild its empire by returning to Russia's former SU borders. This territorial influence aligns with the perspective of A. Dugin (Dugin, 2017). The author stated that one of the main prerequisites to reaching or returning the power of empire for Russia is to reconstitute its influence in post-Soviet areas, integrating surrounding countries and peoples close to Russia's "civilization". But does Russia have the economic and military means to achieve Putin's designated means?

The economic factor is one of the main constituents of Russia's imperialistic ambitions and Putin's empire. Stable economies create the necessary conditions to invest in spreading influence through "soft power" means, such as pan-Slavic or Russian World ideology, military capabilities, diplomatic initiatives, and strategic partnerships that strengthen the global position. The idea of global, or at least regional, power could seem unattainable without strong financial capabilities and a robust economy.

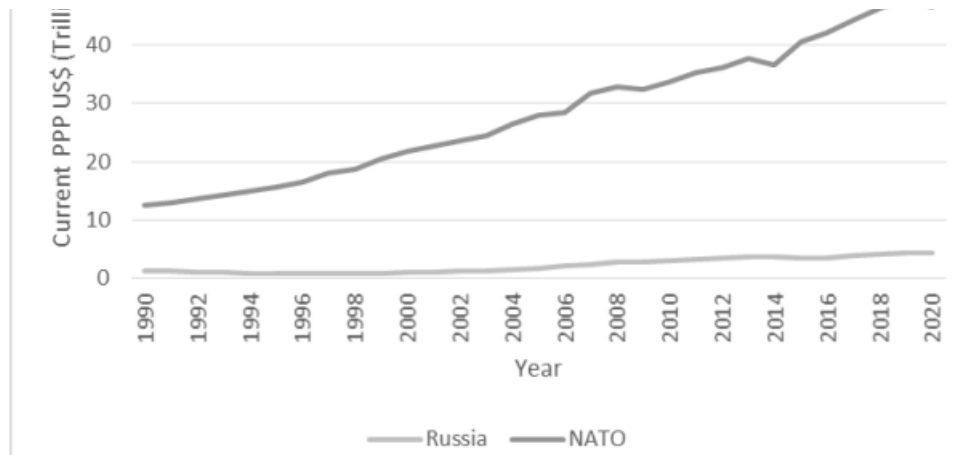
The SU collapsed primarily due to its weak economy and inability to sustain Cold War economic competition. As economic factors are one of the three main factors needed to sustain Russian imperialistic ambition, comparing SU's economic strength with the Russians nowadays is helpful.

Close to the end of the Cold War, the SU covered about 9% of the global population and 10.5% of the global gross domestic product (GDP), as measured by purchasing power parity (PPP). Nowadays, Russia, even together with possible allies (those countries that voted against the UN resolution to stop hostility actions in Ukraine), could represent numbers of 2.5% and 3.5%, respectively (Véron, 2022). The data analysis proves that Russia's economy cannot sustain the same imperial aim as the SU pretended to. Additional arguments supporting this statement could be slow Russian economic progress in the past three decades, dependence on natural resources, and a dim perspective on statistical data.

According to World Bank statistics, Russia is currently one of the eighth largest economies in the world (The World Bank, 2024). However, those numbers represent the total amount of money circling in the country's economy, while the GDP per capita represents the quality of the economy and people's lives. Indeed, compared to the 1990s, Russian prosperity has increased significantly. This is a common trend in developing countries. Therefore, comparing the Russian economy with former subjects and vassals of the SU or neighbours is useful. Among the former Soviet satellites, not only the Czechs and the Hungarians but even the Romanians are more than twice ahead of the Russians in terms of the country's GDP per capita. In 2022, only one country of the former Soviet bloc—Bulgaria—was still slightly behind Russia in GDP per capita, according to the PPP. The GDP per capita result of the Baltic countries that moved from the SU to the European Union is even more insulting and is three times ahead of Russia (The World Bank, 2024).

Furthermore, when looking at the country's GDP as the overall economic capacity, Russia does not rank among the largest countries in the world. It is among the average European countries in terms of financial capacity, slightly ahead of Italy and far behind France and Germany (The World Bank, 2024). Much more drastic differences are seen in Table 2, illustrating the increasing gap between the economic capacity of NATO and Russia.

Table 2. Russia and NATO GDP, 1990-2020 (Current PPP-Adjusted USS)



(Elhefnawy, 2022)

The Russian economy is very reliant on energy resources and materials. The total worth of the country's oil, gas, and other resources represents 60–70 percent of its GDP, depending on the particular year (Cooper, 2013). The country can accumulate significant incomes from their natural resources and invest in their needs, but this income depends on world prices and overall OPEC countries' agreements. Russia can still sustain the same income while suffering from Western sanctions. Nevertheless, this is possible only by increasing production and redirecting delivery routes ("pivot to Asia") to the east, selling gas and oil from a position of weakness with enormous discounts (Ishii, et al., 2023).

After the Russian invasion of Ukraine and business retreat from the Russian market, it cost ~40% of its GDP, retrogressively affecting all thirty years' worth of investment in the country from abroad. Russian imports are suffering considerable difficulties in obtaining essential inputs, components, and technology from reluctant trading partners, resulting in extensive shortages of supplies inside their economies. Russia is at the end of the country's list (similar in the GDP ratio), looking at medium- and high-technology capability areas such as electronics, computing, telecoms, and pharmaceuticals (Table 3).

Table 3. Russia's medium- and high-technology capability

SITC code	Product group	Russia	China	Brazil	India	Turkey	United States
776	Electronic components	<i>0.02</i>	0.69	0.06	0.07	—	1.13
752	Computer equipment	0.05	2.38	0.32	0.06	0.93	0.71
764	Telecoms equipment	0.06	2.16	0.38	0.06	<i>0.05</i>	0.85
874	Measuring-control apparatus	0.22	0.33	0.15	0.15	<i>0.10</i>	2.15
872	Medical instruments	<i>0.04</i>	0.37	0.20	0.23	0.11	2.07
716	Rotating electric plant	<i>0.21</i>	1.32	0.94	0.40	0.53	0.98
731	Metal-cutting machine tools	0.12	0.27	0.31	0.16	0.16	1.25
721	Agricultural machinery	0.29	0.29	2.45	<i>0.17</i>	0.40	1.58
720	Tractors	<i>0.14</i>	<i>0.14</i>	3.41	0.93	1.56	1.27
792	Civil aircraft, spacecraft	0.32	<i>0.07</i>	2.64	.	0.57	3.67
781	Passenger cars	0.06	<i>0.01</i>	0.66	0.17	1.16	0.48
713	Internal combustion engines	<i>0.10</i>	0.19	1.79	0.43	0.98	1.32
541	Pharmaceuticals	<i>0.04</i>	0.67	0.23	0.81	0.12	1.77
821	Furniture	<i>0.11</i>	2.04	0.96	0.28	0.92	0.48

^aItalics = lowest RCA of the six countries; bold = highest.

(Cooper, 2013)

Russia is part of the Eurasian economic cooperation and could create a structure similar to that of the European Union or even be competitive. However, Russia uses the organisation more to spread influence than for economic benefit.

There are no positive perspectives for Russia to build an economy sustaining Putin's ambition to re-establish former SU power. The analysed data, sanctions, and economic outlook make the prospects harmful. Economic well-being, which is based on the export of natural resources, depends on external factors, such as the situation of the sales markets. Prices and recipients are increasing now, but if only the cyclical economy or Asia's favouritism for Russia's resources changes, it will drastically affect Russian incomes. A simple conclusion can be drawn: the economy of the country that occupies one-seventh of the world's land area seems to be at the same level as any medium-sized European country. It can't reflect the strength of former empires.

Following the collapse of the SU, Russia is still trying to maintain its influence through a military prism. Considering a country's military power as one of the main factors in expanding imperialistic influence, it is crucial to analyse the quantities and qualitative aspects.

Some of the former Soviet bloc countries have already joined NATO, and Ukraine will very likely be part of this alliance after the war ends. Therefore, it is helpful to compare Russia's and the NATO countries' military capabilities, which Russia has to overcome to restore the former SU's borders. There is a significant disparity in the military capabilities of the two parties under comparison.

First, military expenditures show the gulf between NATO and Russia's military spending. The disproportion of spending between 1992 and 2020 is stable for the entire period. Taking as an example the year 2019, NATO countries have spent approximately 26 trillion U.S. dollars on their armed forces, comparable with Russia's 1.3 trillion for the same year period (Elhefnawy, 2022). Every year, NATO countries spend twenty times more. Therefore, with its capabilities, Russia can't be aligned with NATO.

Second, Russia's current military capabilities are less robust and capable than the combined military strength of the SU and Warsaw Pact partners (Table 4). Moreover, after the SU collapse and the Warsaw Pact's disintegration, Russia cannot physically compensate for the losses in military capabilities. At the same time, NATO is only expanding and now includes more countries with new, modern capabilities (Table 5). The data analysis indicates that Russia is not only unprepared for aggressive military action in the European region to regain SU territory, but even threats of military force could sound frivolous.

Table 4. Select Indicators of Warsaw Pact Forces (1982) and Russian Forces

	1982	2017
	Warsaw Pact ¹	Russia ²
Total active duty personnel ³	4,000,000	831,000
Divisions	173	9
Motorized rifle brigades	n/a	19
Misc. aviation brigades	n/a	3
Misc. brigades	n/a	18
Artillery regiments	n/a	1
Misc. aviation regiments	n/a	16
Misc. regiments	n/a	1
Main battle tanks	42,500	2,950
Artillery/mortars	31,500	5,317
APCs and IFVs	78,800	13,132
Helicopters	1,700	937
Attack	700	348
Transport/support	1,000	589
Combat-capable aircraft	7,240	1,251
Fighter-bomber/ground attack/ interceptor	6,640	974

(NATO and the Warsaw Pact Force Comparison, 1982)

Third, an essential qualitative aspect to compensate for NATO outnumbering Russia. Michael Kofman and Rob Lee (2022) analyse the most critical compromises regarding the reforms and design of the Russian armed forces. The authors claim that the last reforms in the Russian military prepared it for short and intense warfare based on the heavy use of artillery. However, it is poorly anticipated for a prolonged war of attrition. Military experts have concluded that Russia's main army weakness is its military personnel and their proficiency. Conscription has always been Russia's primary source of military manpower. But what about the professionalism behind it? According to West Point's Modern War Institute's recent assessment (Brimelow, et al., 2022), the leading Russian army weaknesses are logistic failures and the inability to conduct effective combined arms and joint operations caused by a lack of training and combat experience. Soldiers are poorly led and do not have a non-commissioned officer corps with mission command empowerment for subordinate leaders (Johnson, 2022). To conclude, the lack or absence of professional trainers causes the outcome that Russian soldiers are not adequately trained for complex military activities, which are essential nowadays.

Table 5. Select Indicators of NATO Forces in Europe (1982 and 2017)

	1982 ¹		2017		
	NATO ²	U.S. in Europe	NATO	U.S. in Europe	NATO Eastern Flank (Estonia, Latvia, Lithuania, Poland)
Total active duty personnel ³	2,600,000	273,729	1,856,057	63,400	296,040
Divisions	84	4	16	—	3
Mechanized brigades	—	2	47	—	2
Motorized rifle brigades	—	—	—	—	—
Light brigades	—	—	12	—	3
Motorized infantry brigades	—	—	13	—	1
Armored brigades	—	1	16	—	—
Armored brigade combat teams (rotational) ⁴	n/a	n/a	1	1	1
Combat aviation brigades (rotational) ⁵	n/a	n/a	1	1	1
Misc. aviation/airborne brigades	—	—	18	2	3
Misc. brigades	—	1	23	—	—
Artillery regiments	—	—	13	—	—
Misc. aviation regiments	—	—	8	—	—
Misc. regiments	—	2	12	1	—
Misc. infantry battalions	—	—	15	—	—
Artillery/tank battalions	—	—	6	—	—
Misc. battalions	—	—	18	—	1
Main battle tanks ⁶	13,000	3,000	7,101	200	1,075
Artillery/mortars ⁷	10,750	NR	19,272	100	1,299
APCs and IFVs ⁸	30,000	NR	24,265	200	2,946
Helicopters ⁹	2,200	NR	3,301	137	265
Attack	400	NR	430	48	32
Transport/support/ASW	1,800	NR	2,871	89	233
Combat-capable aircraft	2,975	770	2,537	—	98
Fighter-bomber/ground attack/interceptor	2,690	663	2,307	136	98

(NATO and the Warsaw Pact Force Comparison, 1982)

The Russian armed forces can be characterised as having limited military capabilities. Near-sighted military reform and ignoring qualitative aspects opened the Russian military's inability to set against a strong military organisation like NATO, even against one brave country. The conflict in Ukraine has revealed that the perceived might of the Russian military, as documented in official records, does not necessarily reflect effective combat capabilities. Although the Russian military may enhance its

proficiency through practical experience, it is unlikely to pose a significant challenge to NATO forces in the foreseeable future.

Conclusions

This paper has proved the hypothesis that Russia has no military, economic, social or other resources to sustain its imperialistic ambitions over Ukraine or Belarus. To achieve this aim, an analysis of the mentioned capacities was conducted by examining the cases of so-called Pan-Slavic Union imperialism and Putin's attempts to re-establish the SU as efforts to create "Putin's Empire".

The research paper discussed Russia's ability to sustain social-political influence in core Slavic nations and its position as a protector and advocate of Slavic interests. The analysis revealed the relationship between Pan-Slavism, considering its historical context and present-day expressions in its relations with Belarus and Ukraine. In the second part, the Russian fourth wave of imperialism and Putin's attempts to re-establish the SU were analysed from an economic and military perspective. Based on the analysis, this study provided conclusions and potential projections regarding Russia's regional power. By examining the complex interplay of these factors, research brought a comprehensive understanding of whether Russia has the proper political means to sustain its imperialistic ambitions, and these are the main takeaways:

1. The Russian Empire underwent four evolutionary steps. First, during the 16th century, the Tsarist Russian Empire initiated Russian imperial political practices and established the imperial legacy, providing a solid foundation for its imperialistic aspirations. Second, the Romanov dynasty significantly expanded Russia's physical boundaries and geopolitical power. Third, imperialistic traditions persisted into the 20th century with the establishment of the Soviet Empire. Russia's imperialistic ambitions have been a recurring theme throughout its history, and we are victims of what Zaporozhchenko (2023) called "Imperial inertia" and of the efforts and attempts to create the fourth wave of the Russian Empire—the "Putin Empire".

2. Pan-Slavism, in contrast to nationalism, aims to go beyond individual national identity with a broader, "pan-national" identity, including a physical territory larger than just the existing nation-state area. The collapse of the SU pushed back Russia as the

Slavic-centric country capable of keeping power in the core Slavic countries such as Ukraine and Belarus.

3. The classic concept of "Pan-Slavism" now appears outdated, a utopian ideology that belongs more to the pages of history books than the modern world. Ukrainians no longer needed Pan-Slavic ideas, mainly after Russia used them to justify its imperial expansion. And there is substantial dissent in Belarussian society and among elites.

4. Belarus, balancing its identity and alliance with Russia and between the West and the East in foreign policy, pursues more pragmatic goals and benefits for the regime. Pan-Slavic ideas are more declarative than reflecting the will and efforts aimed at the reunion with Russia or creating any pan-Slavic union.

5. The Putin regime has shown its ability to adjust its ideology to different audiences, using the Eurasianist, Rossiya, or Russian World terminus. However, the ability to develop and sustain is limited as the spread of pan-Slavic ideas is no longer appealing.

6. There is a remarkable transition of identities with the significant effort to distance from Russian influence within the so-called pan-Slavic core nations. Consequently, Pan-Slavism or any other ideas that once inspired Slavic nations to seek closer cooperation appear void.

7. The SU GDP was 2.5 times larger than Russia's economic capabilities nowadays. The economy of a country occupying one-seventh of the world's area is at the same level as that of a medium-sized European country like Italy. Therefore, there are no prerequisites for Russia's economic capabilities to seek and sustain the same imperial aims as the former SU pretended to do using economic instruments of power.

8. Comparing the military capabilities of Russia and NATO countries, which Russia must overcome to restore the borders of the former SU and create the Putin Empire, there is a vast difference in the military capabilities of those two comparing parties in favour of NATO:

- a. NATO military spending has been twenty times bigger than Russian in the past three decades.
- b. NATO outnumbers Russia in all aspects of military equipment.

- c. Near-sighted reform of the military and ignoring qualitative aspects discovered the Russian military's inability to set against not only a strong military organisation like NATO but even one brave country.

Considering the arguments above, the author of the research paper would like to suggest the following recommendations. Firstly, expanding the understanding of Russia's imperial nature, inertia, and periodical attempts to restore the empire at any cost is essential. This ideological root for conflicts must be the basis for strategic planners - a starting point for a global policy to deter and contain Russia.

Secondly, it is essential to maintain Russia's limited ability to strengthen political means to achieve imperial goals. This will be achieved by strengthening the integration process of national communities, especially in post-Soviet states. Stressing the connection with the country of residence and moving away from any form or expression of Pan-Slavism or Russian World ideas is crucial. Moreover, Russia's global economic isolation will limit its economic and technological development growth. In addition, a strong position on deterrence, NATO resolve, and unity will leave no room for Russia to regain the former SU's territorial boundaries.

Lastly, to the greatest extent, support and development of democratic values among the people of Russia and its neighbours have to take place, thereby strengthening resistance to Russian narratives in any form.

In conclusion, Russia has not rid itself of its imperialistic ambitions, and the world is observing the wave of Russian imperialism. Putin's efforts and attempts to create a new "Putin Empire" and bring Russia back into the former SU territorial borders with military means are menacing. These aspirations are still influenced by ambition and the historical legacy of the Russian Empire and the Soviet Union ideas. As the research suggests, Russia doesn't have the political means for such ambitions, which makes the Kremlin activities even more unpredictable. In the event of retreating, giving up and risking foreign policy objectives, Russia might apply nuclear power to achieve its imperial ambitions. After all, the empire is not a natural political unit – it rises and inevitably falls. With the freefall, Putin might act irrationally with global consequences. Therefore, all near, middle and long-term future attempts and efforts to restore the empire are bound to fail, but the West must view them with utter caution.

Bibliography

Bikanau, Philipp and Nesterovich, Konstantin . 2023. Analytical Report. Belarusian Identity in 2023: A Quantitative Study. [Online] December 2023. [Cited: 11 January 2024.] <https://library.fes.de/pdf-files/bueros/belarus/20889.pdf>.

Boeckh, Katrin. 2016. The Rebirth of Pan-Slavism in the Russian Empire, 1912–13. [book auth.] Boeckh Katrin and Rutar Sabine. *The Balkan Wars from Contemporary Perception to Historic Memory*. Cham, Switzerland : Springer Nature, 2016.

Brimelow, Benjamin and Shultz, Richard. 2022. Modern War Institute. *Russia's Potemkin army*. [Online] 23 May 2022. [Cited: 11 December 2023.] <https://mwi.usma.edu/russias-potemkin-army/>.

Cohen, Ariel. 1996. *Russian Imperialism: Development and Crisis*. s.l. : British Library Congress Cataloging-in-Publication Data, 1996.

Cooper, Julian. 2013. Eurasian Geography and Economics. *Can Russia Compete in the Global Economy?* [Online] 15 May 2013. [Cited: 1 March 2024.] https://www.researchgate.net/profile/Julian-Cooper-2/publication/250171694_Can_Russia_Compete_in_the_Global_Economy/links/5711ef3908aeff315b9f80ba/Can-Russia-Compete-in-the-Global-Economy.pdf.

Đorđević, Vladimir, et al. 2023. Cambridge University Press. *Revisiting Pan-Slavism in the Contemporary Perspective*. [Online] 19 August 2023. [Cited: 16 October 2023.] <https://www.cambridge.org/core/journals/nationalities-papers/article/revisiting-panslavism-in-the-contemporary-perspective/4EA532EFCBF0F66ACBBE6EBEF34B374C>.

Đordoević, Vladimir, et al. 2021. Beyond Contemporary Scholarship and toward Exploring Current Manifestations of Pan-Slavism. *Canadian-American Slavic Studies*. 55(2), 2021, Vols. 147–159.

Dugin, Aleksander. 2017. *The rise of the fourth political theory*. United Kingdom : Arkos Media Ltd, 2017.

Elhefnawy, Nader . 2022. SSRN. *NATO and Russia: A Note on the Military-Industrial Balance*. [Online] 29 November 2022. [Cited: 8 November 2023.] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4288547.

Federation, The Ministry of Foreign Affairs of the Russian. 2023. *The Concept of the Foreign Policy of the Russian Federation*. [Online] 31 March 2023. [Cited: 14 November 2023.] https://mid.ru/en/foreign_policy/fundamental_documents/1860586/.

Grikontas, Robertas. 2018. Rusų pasaulio ideologemos funkcija – stiprinti imperinę tapatybę (The function of the ideologeme of the Russian World is to strengthen the imperial identity). [book auth.] Arūnas Bubnys. *Genocidas ir rezistencija*. Vilnius : Lietuvos gyventojų genocido ir rezistencijos centras, 2018, pp. 42-70.

Ishii, Karine , Macaire, Camille and Stalla-Bourdillon, Arthur . 2023. Banque de France. *China has reduced its energy bill thanks to Russian oil discounts*. [Online] 7 Sep 2023. [Cited: 14 November 2023.] <https://www.banque-france.fr/en/publications-and-statistics/publications/china-has-reduced-its-energy-bill-thanks-russian-oil-discounts>.

Johnson, David. 2022. Would we do better? Hubris and validation in Ukraine. [Online] 31 May 2022. [Cited: 29 February 2024.] <https://warontherocks.com/2022/05/would-we-do-better-hubris-and-validation-in-ukraine/>.

Kofman, Michael and Rob, Lee. 2022. War on the rocks. *Not built for purpose: the Russian military's ill-fated force design*. [Online] 2 Jun 2022. [Cited: 1 November 2023.] <https://warontherocks.com/2022/06/not-built-for-purpose-the-russian-militarys-ill-fated-force-design/>.

Mankoff, Jeffrey. 2022. The War in Ukraine and Eurasia's New Imperial Moment. [Online] 2022. [Cited: November 7, 2023.]. [Online] 14 July 2022. [Cited: 24 November 2023.] https://bpb-us-e1.wpmucdn.com/blogs.gwu.edu/dist/1/2181/files/2022/07/Mankoff_45-2_TWQ-1.pdf.

—. 2022. The Washington Quarterly. *Empires of Eurasia: How imperial legacies shape international security*. New Haven and London : Yale University Press, 2022, pp. 16-60.

NATO and the Warsaw Pact Force Comparison. 1982. NATO home page. *The Cold War: Defence and Deterrence*. [Online] 1982. [Cited: 17 January 2024.] https://www.nato.int/cps/en/natohq/declassified_138256.htm.

O'Loughlin, John and Toal, Gerard . 2022. Post-Soviet Affairs. *The geopolitical orientations of ordinary Belarusians: survey evidence from early 2020*. [Online] 21 March 2022. [Cited: 28 February 2024.] https://www.tandfonline.com/doi/pdf/10.1080/1060586X.2022.2030126?casa_token=CAXe1PWAs0wAAAAA:2Db6jp-fbu4Qn3FGUOZIT0IH4QfUakQXdm1WTPAYZ8kAGIKITFE0ikD47IBRsQoTjc6DizYnRoBDYA.

Olszanecka, Natalia. 2021. History and Politics. *Future War: The Russian Perspective*. [Online] 1 Jun 2021. [Cited: 11 December 2023.] <https://apcz.umk.pl/HiP/article/view/36113>.

Policy Meeting on the Implementation of Historical. 2022. President of the Republic of Belarus. *Soveshchanie po voprosam realizatsii istoricheskoi politiki [Meeting on the implementation of historical policy]*. [Online] 6 January 2022. [Cited: 10 January 2024.] <https://president.gov.by/ru/events/soveshchanie-po-voprosam-realizacii-istoricheskoy-politiki>.

Putin's Munich Speech . 2015. Putin's famous Munich Speech 2007. [Online] 20 November 2015. [Cited: 16 October 2023.] https://www.google.com/search?sca_esv=589538557&rlz=1C1KNTJ_enLT1007LT1007&sxsrf=AM9HkKIHS-gNQxKOVj66V3x94IzSvw7m7A:1702203995499&q=Putin%27s+2007+Munich+Secu

city+Conference+speech&tbm=vid&source=lnms&sa=X&ved=2ahUKEwjSnPKD1ISD
AxULbvEDHb0YBSQQ0pQJegQICxAB.

Sanborn, Joshua A. 2014. Taylor and Francis Online homepage. *RUSSIAN IMPERIALISM, 1914–2014: ANNEXATIONIST, ADVENTURIST, OR ANXIOUS?* . [Online] 19 November 2014. [Cited: 4 October 2023.] <https://www.tandfonline.com/doi/full/10.1080/09546545.2014.973677>.

Sonnenfeld, Jeffrey. 2022. Yale school of management. *Business Retreats and Sanctions Are Crippling the Russian Economy*. [Online] August 2022. [Cited: 02 March 2024.] <https://dariendma.org/wp-content/uploads/Russian-Economic-Impact-Slide-Deck-August-2022-v6-1.pdf>.

Suslov, Mikhail. 2013. Geographical Metanarratives in Russia and the European East: Contemporary Pan-Slavism. [Online] May 2013. [Cited: 20 October 2023.]. [Online] 15 May 2013. [Cited: 12 November 2023.] <https://www.tandfonline.com/doi/abs/10.2747/1539-7216.53.5.575>.

Suslov, Mikhail, Čejka, Marek and Đorđević, Vladimir . 2023. *Pan-Slavism and Slavophilia in Contemporary Central and Eastern Europe: Origins, Manifestations and Functions*. Cham : Springer Nature Switzerland AG, 2023.

The World Bank. 2024. World Bank national accounts data, and OECD National Accounts data files. [Online] 2024. [Cited: 11 01 2024.] https://data.worldbank.org/indicator/NY.GDP.MKTP.CD?most_recent_value_desc=true.

Véron, Nicolas . 2022. *Thoughts, articles and references on business, finance, public life, and more*. [Online] 8 April 2022. [Cited: 14 January 2024.] <https://www.nicolasveron.info/main/2022/04/putins-russia-is-a-minnow-compared-to-the-cold-war-soviet-bloc.html>.

Véron, Nicolas. 2022. Putin's Russia is a minnow compared to the Cold War Soviet Bloc. [Online] 2022. <https://www.bruegel.org/blog-post/putins-russia-minnow-compared-cold-war-soviet-bloc#:~:text=At%20the%20end%20of%20the,are%202.5%25%20and%203.5%25..>

Zaporozhchenko, Ruslan. 2023. The End of "Putin's Empire?" Ontological Problems of Russian Imperialism in the Context of the War against Ukraine. [Online] 5 January 2023. [Cited: 16 October 2023.] www.tandfonline.com/doi/full/10.1080/10758216.2022.2158873.

TAAVI KAROTAMM. Is Estonia Ready to Involve Unorganized Support from Civil Population to National Defence as has Ukraine?

Introduction

Past decades have shown that although the Cold War was believed to be over, Russia's imperialist ambitions have not ceased. Cyber-attacks against Estonia (2007), the invasion of Georgia (2008), the illegal annexation of Eastern Ukraine (2014), a full-scale invasion of Ukraine (2022), and other similar events show that countries neighbouring Russia cannot feel safe and need to prepare to defend themselves with all possible means and resources. The need for using a nationwide defence model applies especially to small countries such as Estonia that cannot afford, financially and societally, full-time active-duty armed forces of sufficient size to defend against an adversary of a significant size as Russia.

War in Ukraine has lasted for over ten years, with more than two years having passed since the full-scale invasion on 24 February 2022. These years have offered an invaluable opportunity to learn from a country fighting Russia, which is seen as a significant threat to NATO and its members (Stoltenberg, 2022). However, have the lessons, often paid for with Ukrainian blood and lives, been identified and learned, or neglected and ignored?

This research paper (RP) aims to evaluate the preparedness of Estonian comprehensive approach to national defence, in the framework of the Ukrainian experience in involving unorganized voluntary support to armed resistance from the civil population during the first two months of the full-scale Russian invasion (February to April 2022).

This research is expected to answer the following research questions:

- Is resistance by civil population relevant in case of an intrusion by a foreign military?
- To what extent has the Estonian defence sector (Estonian Defence Forces, Estonian Defence League) prepared to accept and involve unorganized voluntary civil

assistance to armed resistance based on examples from Ukraine from February to April 2022?

In this research paper, Estonian security environment and approach to national defence are being assessed, followed by a theoretic overview of involvement of civil population in defence activities. Supported by research regarding the role of civil population in defence of Ukraine in 2022, an understanding of the relevance and roles of civilians in case of an intrusion is built. Estonian readiness to utilize such support as seen in Ukraine is assessed based on interviews with the Commander of Estonian Defence Forces and (now the former) Commander of Estonian Defence League. As the result of the research, an assessment about the status, and recommendations for future involvement of civil population are given.

The content of this research paper is limited by the requirement of being Unclassified, resulting in the use of only public material.

Methodology

The theoretical part of the RP is based on the theories of resistance and special operations. Additionally, the Estonian National Defence Policy and Comprehensive Approach to National Defence will be described to assess Estonian plans to involve civilian population to support armed resistance against an invasion.

For analysing the readiness of involving the civil population to support resistance based on experience from Ukraine, qualitative analysis of data from both primary and secondary sources is being used. Ukrainian experience is mapped based on unstructured interviews with senior officers of the Armed Forces of Ukraine (AFU) that requested anonymity while providing the answers. This data is supported and supplemented by public sources. The aim of this section is to describe the support provided to AFU by civil population in Ukraine.

Based on the Ukrainian experience, structured interviews with evaluative and descriptive questions were conducted with commanders of Estonian Defence Forces (EDF) and Estonian Defence League (EDL). This section aims to form an understanding of how well organizations are prepared to utilize similar support as was seen in Ukraine in 2022.

An analysis of the information gathered during the research was conducted to form a final understanding of Estonian readiness to host similar unorganized voluntary support as was provided to AFU in the first months of 2022.

Estonian approach to national defence and the security environment

The aim of this chapter is to form the base for understanding the Estonian approach to national defence. Defence model of the Republic of Estonia and overview of the security environment will be described based on relevant official public documentation.

Estonian approach to national defence

Estonian defence is based on two main pillars: individual self-defence capability by the country's own resources and collective defence capability by NATO and its member states (Estonian Ministry of Defence, 2015). Own resources of the country are being described as active duty and reserve members of EDF and EDL, together with other organizations supporting their effort (Defence Resource Agency, Estonian Foreign Intelligence Service, Centre for Defence Investment etc.) (Estonian Ministry of Defence, 2018). However, it is noted by the Ministry of Defence (MoD) that in addition to serving in defence-related organizations, one can also contribute to national defence via voluntary citizen's initiative (Estonian Ministry of Defence, 2023).

Utilization of various national resources and capabilities for defence of the country is also described in the National Security Concept of Estonia, where it is stated that defence of the nation is based on the readiness of each individual, and that all possible military and non-military assets, including private, public and third sector, shall be involved if the country needs to be defended (Government of Estonia, 2023 p. 4).

The society-wide approach is supported by attitudes in the society, assessed in an annual study 'Public opinion on national defence' ordered by the Estonian MoD. In the report of 2023, 'residents' defence willingness' is seen as the third most important security guarantee to Estonia (after NATO membership and allied presence), while 83% of respondents say armed resistance is needed in case of an attack, and 64% of the respondents are willing to participate in that resistance (Eesti Uuringukeskus OÜ, 2023 pp. 30-32). Describing resistance efforts, 11% of respondents would prefer participating in armed defence, while 24% would contribute to defence in auxiliary roles and 30% in non-military activities (Eesti Uuringukeskus OÜ, 2023 p. 35).

Citizens' right to take initiative in national defence is also declared in paragraph 54 of the Estonian Constitution, where it is stated that defending the country's independence is the duty of every citizen and, in case of lack of other means, one can resist a forcible change to the country's constitutional order by taking their own initiative in resisting the attempt (Parliament of Estonia, 1992).

To enhance the possibilities of resisting hostile interventions, a change was made to 'Estonian Defence Forces Organisation Act' (paragraphs 37 and 41-43), allowing EDF to conduct various new tasks, including involvement of people in covert cooperation, in order to prepare and organize armed resistance with members of Estonian society (Parliament of Estonia, 2023).

Estonian defence capabilities

As mentioned prior, main actors in organized armed resistance in Estonia are Estonian Defence Forces and Estonian Defence League. EDF are the main national armed forces, while EDL is a voluntary organization, organized based on military principles and citizens' initiative to contribute to defence of the country (Estonian Defence League, 2023).

Crisis establishment of Estonian Defence Forces consists of approximately 43 000 active duty, reserve, and civilian personnel, supplemented by more than 40 000 reservists that have been trained but are not anymore assigned to positions in crisis establishment (Estonian Defence Forces, 2023). Additionally, Estonian Defence League ('*Kaitseliit*' in Estonian) involves about 18 000 members, or 29 000 together with affiliated organizations (Estonian Defence League, 2023).

Yet, since about 10 000 of the 18 000 members of Estonian Defence League are also represented in the crisis establishment of Estonian Defence Forces (of 43 000 troops) (Estonian Defence Forces, 2023), it can be assessed that initially a total of about 51 000 people (43 000 members of Defence Forces and remaining 8000 active members of Estonian Defence League) are planned to participate in active organized armed defence of Estonia in case of an external threat to the country's independence. Members of affiliated organizations of EDL will participate in unarmed resistance, and the trained

reservists without wartime assignments can be assigned and called into duty if they meet the standards of standing regulations. Composition of EDF and ELD is graphically described in Figure 1:

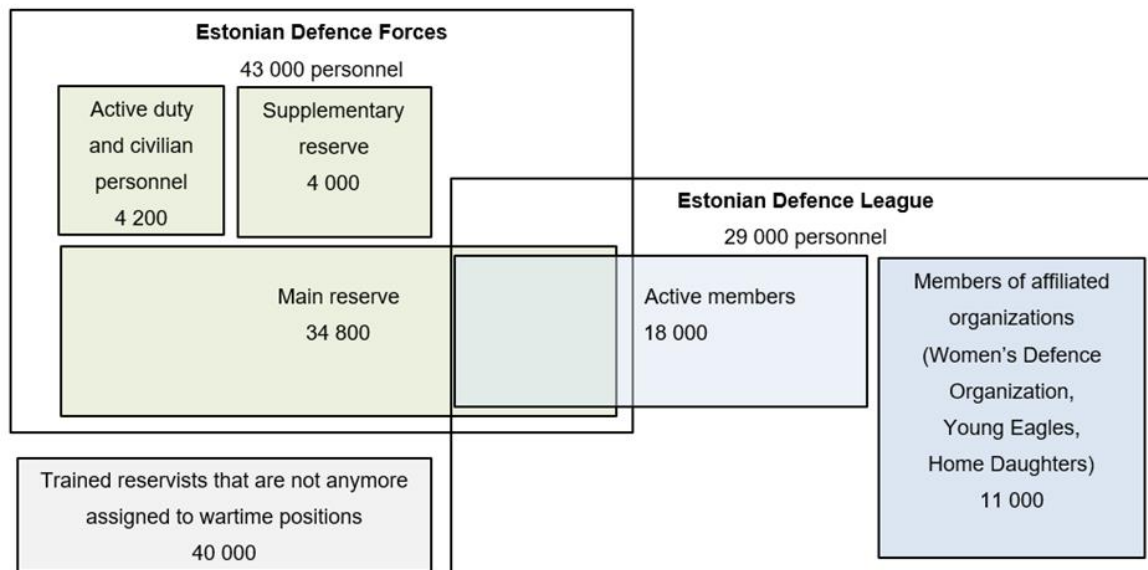


Figure 1 Overview of Estonian defence structures. Source: author, based on websites of EDF and EDL (Estonian Defence Forces, 2023; Estonian Defence League, 2023).

Estonian security environment

The Estonian National Security Concept, approved in 2023, clearly states that the main external threat to the country is Russia. Based on the document, Russian Federation poses an existential long-term threat to Estonia and other countries bordering Russia, since Russian leadership has repeatedly proven that they are not hesitant to use various levers of influence, including military and warfare, to pursue their national aims (Government of Estonia, 2023 p. 6).

Despite having encountered significant losses in Ukraine, even the remaining assets of Russian Armed Forces still pose a threat to smaller members of NATO, such as Estonia and other Baltic states. Prior to 24 February 2022, Russia had permanent presence of about 19 000 troops close Estonian borders (6. Combined Arms Army and 76. Air Assault Division) (Estonian Foreign Intelligence Service, 2023 pp 11, Estonian Foreign Intelligence Service, 2024, pp 17) that could have been increased by attachment of other units or involvement of reserve troops (Military Intelligence Center, Estonian Defence Forces, 2021 pp. 10-11). Additionally, Russia is planning to reform its military units in the Baltic region by 2026, with splitting the Western Military District up to Leningrad and Moscow regions, as well restructuring some of its brigade level

units to division level units (Military Intelligence Center, Estonian Defence Forces, 2023).

Yet, restructuring units does not necessarily provide a qualitative effect in the short term, since Russian units are engaged in Ukraine, bearing significant losses amongst manpower and equipment during the writing of this RP. However, Estonian Foreign Intelligence Service has assessed that, in up to four years, Russian capabilities near Estonian borders can be reconstituted and risk to Baltic states would increase significantly, especially in case of Russian success in Ukraine (Estonian Foreign Intelligence Service, 2023 pp. 11-12). Russia has also the ability to significantly increase their presence under the cover of exercises, as was demonstrated in January 2022 when they amassed about 120 000 troops to the Ukrainian border (Wasielewski, et al., 2022), increased to up to 190 000 troops by February 2022 (Brown, 2022).

Therefore, it can be concluded that despite the losses that the Russian forces have encountered in Ukraine, they still have the capability to influence the Baltic nations today, as well ambitions to restore and increase their capabilities by 2026. Due to previous offensive behaviour by Russian Federation towards its neighbours and the ability to also amass significant military resource from other military regions, countries sharing borders with Russia cannot feel safe. Instead, nations need to prepare and utilize all resources to defend themselves. In the Estonian context, the roughly 50 000 troops planned to be utilized in the defence of the country is not a significant amount, especially considering the vast need to replace casualties. From that perspective, support should be obtained from, and possibility some tasks to be fulfilled by, civil population.

Involvement of civil population

As concluded before, civil population needs to be involved in defence of Estonia in case of a threat. One way to frame the involvement of civilians, leaving aside the conventional mobilization of reservists, is via resistance, that the U.S. Department of Defence (DoD) has defined as *'an organized effort by some portion of the civil population of a country to resist the legally established government or an occupying power and to disrupt civil order and stability'* (U.S. Department of Defence, 2016 p. 204).

In the definition by the U.S. DoD and in the context of this paper, the part of civil population resisting an occupying power is the key. The organized portion of the definition refers to, in Estonian case, members of EDL. Simultaneously, there is the unorganized part of volunteers that are currently not members of EDF/EDL but, in case of war, would start providing their assistance.

In the Resistance Operating Concept (ROC), published by Joint Special Operations University (JSOU), resistance is defined in a similar manner, but distinction between violent and non-violent resistance has been made: *'a nation's organized, whole-of-society effort, encompassing the full range of activities from non-violent to violent, led by a legally established government (potentially exiled/displaced or shadow) to re-establish independence and autonomy within its sovereign territory that has been wholly or partially occupied by a foreign power'* (Fiala, et al., 2020). Therefore, it is important to distinguish between violent and non-violent activities.

Resistance is, by the perspective of the U.S., part of Unconventional Warfare (UW), one of the core activities of Special Operations (U.S. Department of Defence, 2014 pp. II-3). While NATO has not included resistance in its Special Operations doctrine, resistance is still mentioned as part of UW in NATO's Glossary of Terms and Definitions (NATO Standardization Agency, 2013 pp. 2-U-1) and in the Comprehensive Defence Handbook (2020) by the NATO Special Operations Headquarters (NATO Special Operations Headquarters, 2020).

The need for involving civilians in national defence has also been recognized by Ukraine that has released a handbook 'Civil resistance in occupied territories', instructing civil population to conduct various activities for violent and non-violent resistance (Special Operations Force of Ukraine, 2022).

From the perspective of the Comprehensive Defence Handbook, there are 4 layers that national defence should be based on: 1) individual resilience, 2) official defence and security organizations, 3) Home Guard supported by civic and private sector and 4) Asymmetric Defence Component (NATO Special Operations Headquarters, 2020 pp. 34-35). In the context of this research, the most relevant layer seems no. 3

regarding Home Guard (*Kaitseliit* in Estonian context) and civic support by volunteers, but not only to *Kaitseliit*, but in a broader sense to the whole of national defence.

However, the role of individual resilience and Asymmetric Defence Component (ADC) are also essential for a successful defence. The ADC can be seen as extra fighters, usually voluntary members of society that are prepared prior to the crisis, that support the resistance effort either under the command or on the side of official national forces (NATO Special Operations Headquarters, 2020 p. 48).

Volunteers can also be part of the Auxiliary groups providing support (material, labour, intelligence collection, early warning, communications, safe house management, logistics etc), to the ADC and official defence structures. However, prior background checks, assimilation to networks and training might be required based on the roles and assignments (NATO Special Operations Headquarters, 2020 pp. 46-49).

NATO Comprehensive Defence Handbook brings also out the possible functions and organizations of private- and civic sector that could contribute to defence. Amongst other possible contributions communications, transportation, printing services, supplying food and water, financial and material support, facilities, construction, cyber and medical assistance have been listed (NATO Special Operations Headquarters, 2020 pp. 52-54, 58). Therefore, NATO mainly sees volunteers as the non-violent force. It is important to note that a selection of the tasks described for ADCs and Auxiliaries in the NATO Handbook and ROC are also brought out in the Ukrainian civil resistance handbook. While NATO guidance suggests the need for prior organizing and training of the ADC and Auxiliaries, Ukrainian approach also accepts contribution by non-trained non-organized volunteers and this both for non-violent and violent resistance (Special Operations Force of Ukraine, 2022). Volunteers have also been involved in the Asymmetric Defence Component, conducting acts of sabotage (Special Operations Force of Ukraine, 2022 pp. 10-18), attacking enemy with self-made Molotov cocktails (General Staff of Armed Forces of Ukraine, 2022) and other means.

The following table describes the classification of different actors participating in resisting the invasion based on the Estonian example.

Classifications of population participating in resistance				
Level of organization	Organized			Unorganized
Classification in official documentation	Members of official military organizations	Asymmetric Defence Component/ Armed component/ Guerillas	Auxiliary forces	Civil society
Training and membership of organizations	Trained and members	Trained and members, or part of a pre-established network	Trained and members, or part of a pre-established network	Non-trained, non-members
Type of resistance	Violent	Violent	Non-violent	Non-violent
Classification by EDL	Fighters	Fighters	Amplifiers	Enablers
Role	Resist the enemy	Resist the enemy	Support the fighters	Support the fighters
Example in Estonian case	Member of EDF/EDL with a war time role.	Organized groups of population prepared to resist the enemy, such as fighting groups of the EDL or members of an EDL-coordinated network.	Members of EDL or suborganizations without a war time position. Members of an EDL-coordinated network.	Business owner, drone enthusiast, hobby radio specialist, tractor owner, chef etc with no war time task and not official connection to EDF/EDL.

Table 1. Classification of members of the society based on their role in national defence. Source: author, based on (Keiley-Listermann, et al., 2019; Fiala, et al., 2020; NATO Special Operations Headquarters, 2020; Ühtegi, 2023a).

The variety of actors described in Table 1 will make Estonia a confusing battlefield not only to own troops, but as well to Allies that need to distinguish the neutral members of civil society, friendly population that is supporting the resistance, Auxiliaries and ADC from the hostile population and unconventional enemy troops. To reduce potential confusion and frictions, ways of distinguishing between parties needs to be planned. In the context of this research, unorganized, non-trained non-members of defence organizations will be focused on as volunteers since the involvement of other parties is already being planned and exercised by the EDF and EDL. It seems that the support from unorganized part of the society in Estonia might not be accounted with, while in Ukraine they played a critical role. Therefore, involvement of this part of the society will be examined further.

To sum up, it can be concluded that Estonia needs involvement of civil population to its national defence. Estonian military resources are not sufficient to counter adversary as large as Russia and therefore, even when fighting together with its NATO allies,

Estonian population needs to, and could contribute to, defending the country. This approach has been partially described in Estonian defence related documentation, and it is supported by experience from Ukraine where civil population took part in resisting Russian invasion, as well by U.S. and NATO doctrines that describe civil resistance as a tool for countering an adversary. Next chapter of the research will map the ways Ukraine has utilized voluntary support to its armed forces and will assess whether Estonia is prepared for similar involvement of volunteers.

Ukrainian experience and Estonian preparations

The following chapter will describe support to armed resistance by the civil population in Ukraine and Estonian readiness to accommodate similar efforts.

Ukrainian experience

Based on the interviews with representatives of AFU, supported by research of publicly available material, civil population offered AFU a great variety of support right from the beginning of the full-scale invasion (Sheth, 2022; Senior officers of the Armed Forces of Ukraine, 2023).

All interviewees agreed that spontaneous unorganized civil support was critically helpful and necessary especially in the first weeks after the full-scale invasion since it supplemented and even filled gaps in AFU-s capabilities. Such support also increased the speed at which Ukraine achieved its readiness to resist Russia.

Interviewees listed over 20 ways of civil support that they had noticed. Yet, the list is not ultimate, since the feedback from the officers and publicly available data most likely does not provide information on all the activities of civil support. The main activities conducted by the population were regarding:

- collection of information (enemy locations, movement, air attacks, situation, damage assessment),
- organizing support (equipment, supplies, ammunition, funds, synchronization of volunteer activities),
- building and producing (equipment, fortifications, barricades, obstacles, improvised explosives, digital platforms, deployment areas and storages, modification and repair of equipment) and,

- conducting active operations against the enemy (hacking, information dissemination, intimidation and demoralization, denial of movement, non-compliance, obtaining enemy equipment and supplies, patrolling, disorienting the enemy, lethally engaging the enemy, exposing and hunting traitors, exposing and intimidating collaborators, seeking and eliminating small enemy groupings).

A detailed list of civil support to AFU, based on interviews and public material, is in the possession of the author.

Estonian readiness

The list of support provided to AFU was used as exemplary possibilities of civil support during interviews with General Martin Herem (Commander of Estonian Defence Forces) and Major General Riho Ühtegi (Commander of Estonian Defence League) on 24 November 2023. Full results of the interviews are in possession of the author. Key takeaways and overall conclusions drawn from the interviews are described in the upcoming paragraphs.

Estonian Defence Forces foresee a high need for involving assistance from civil population (rating '5' at a scale of 1-5), however the readiness of the organization to do so was described as minimal (rating '1' at a scale of 1-5) (Herem, 2023). As per General Herem, the organization has done a lot to prepare for utilizing civil support, yet a lot could be done more, better and in more detail.

An important consideration that differentiates Estonia from Ukraine was mentioned to be the role and preparedness of Ukrainian territorial defence units that should have fulfilled some of the tasks that were conducted by civil population. The development of territorial defence system in Ukraine had not yet reached strong results by the full-scale invasion in 2022, while the system in Estonia ('*Maakaitse*') has been developed and tested already for years for, amongst other matters, involvement of civil support. Therefore, many of the tasks conducted by civil population in an uncoordinated manner would in Estonia be more coordinated and often carried out in cooperation between civil population and territorial defence units (Herem, 2023).

Based on General Herem, most of the assistance by civil population ought to be coordinated at the lowest possible level, meaning even platoon level, to ensure speed and best use of local resource. This is also due to the reason that this way local units

sustain the best situational awareness of their area of responsibility, which is necessary also for allied troops that shall be involved in defence of Estonia (Herem, 2023). As an example, General Herem mentioned the population-organized roadblocks in Ukraine, that in Estonia could work against the countries defence, since there would be armed forces of multiple countries defending Estonia, whose freedom of movement could be limited by such roadblocks. However, those roadblocks and checkpoints would be useful if their locations were coordinated with local units.

As per the interview with General Herem, not all products that the EDF needs to defend the country must be ready in storages, especially when local companies have the capability to produce them. Therefore, both the EDF and the society should be prepared to shift from peace time to war time. To improve the readiness of EDF in involving civil support, EDF should prepare to use of civil support in detail in advance, including preparation of necessary plans, guidance, and technical descriptions, so that in case of a threat clear, simple, and timely guidelines could be given to local companies and population to direct their supporting activities. Currently, the level of preparedness of such documentation is shallow (Herem, 2023). Additionally, resource that requires longer development, such as digital platforms, should be developed already in peace time so that they would be tested and known for society. For all this to happen, EDF needs to work as a whole, with its members taking more initiative, ownership and responsibility (Herem, 2023).

From the perspective of Estonian Defence League, the gap between the need to involve civil support and readiness of the organization to do so is much smaller than for the EDF, with the need rated by '5' and readiness by '3' (Ühtegi, 2023a). While the need is again undoubted, the reason for rating the readiness with '3' is mostly said to be, based on General Ühtegi's assessment, due to legislative matters that limit their peace time cooperation with partners and involvement of personnel, and does not give specific role or guidance for war time. The biggest strength of EDL, that would enable rating the readiness with '4', is the organization's way of operating, meaning that a lot of the resource, approaches and networks are already in use and tested in everyday settings and exercises (Ühtegi, 2023a).

As General Herem, General Ühtegi also supports the approach of utilizing as much support from civil population as possible, with the majority of activities being

coordinated at the lower levels of territorial defence units. Both generals also assessed that some activities, such as cyber operations or providing guidance for general population, should be coordinated at higher levels (meaning HQ level of EDF or EDL, or at a command level such as Cyber Command) (Herem, 2023; Ühtegi, 2023a).

During his interview, General Ühtegi stated that *'War is more than just an armed fight, and therefore all can contribute even without firing a weapon.'* Former commander of EDL sees the role of Estonian population during the war as fighters, amplifiers, and enablers (in Estonian *'võitlejad'*, *'võimendajad'*, *'võimaldajad'* (Ühtegi, 2023b)), while the rest of the population contributes to keeping the society and critical services operational (Ühtegi, 2023a). Based on the concept of fighters-enables-amplifiers, fighters are trained to engage the enemy, amplifiers are members of EDL that are able, but not specifically trained to fight the enemy and are not assigned a war time position (also can be seen as 'auxiliary forces' (Fiala, et al., 2020 p. 13)) and enablers are organizations and members of the population that support the fighters and amplifiers (Ühtegi, 2023a; Ühtegi, 2023b).

Both General Herem and General Ühtegi agreed that due to the small size of Estonia, support from the population, organizations and businesses is needed for effectively defending the country. That support, however, needs to be preplanned and coordinated to bring the best results (Herem, 2023; Ühtegi, 2023a).

To summarize, the experience from Ukraine shows that during the beginning of the full-scale invasion, the civil population provided the armed forces of Ukraine various kinds of support. In Estonia, such support is also appreciated and anticipated, however in a more coordinated manner. The biggest difference between the countries seems to be the readiness of territorial defence forces that should be the link between civil population and armed forces, and coordinator of civil support.

Analysis

Involvement of civil population in national defence has been described in U.S. and NATO doctrines, as well in Estonian defence related documentation. This indicates that society-wide resistance is seen as a credible approach in case of an armed invasion. That applies specially to a country like Estonia that is small in territory, as

well in the numbers of its military personnel. Considering the strength of the Russian forces bordering Estonia, it is vital that all resources of the country, from people to organizations and businesses, contribute to defending the nation.

Based on the interviews with officers of Armed Forces of Ukraine and research of publicly available material, it can be said that civil population provided AFU with various support that contributed to their activities. Local population started assisting right from the beginning of the full-scale invasion and the support covered a wide area of activities that could and should have been conducted also by military forces (denial of movement, patrolling, lethally engaging the enemy, information collection and reconnaissance, transportation, engineer work, equipment repairing and modifying, resupply, cyber activities etc). That shows that AFU units were not able to conduct the activities in a timely manner, and civil population started contributing to supplement the AFU capabilities. Even though Ukraine has a population 33 times larger than Estonia, and its armed forces substantially out-weigh the Estonian Defence Forces in manning and firepower, AFU still required civil support to successfully initiate and conduct its defensive operations. Therefore, it is hard to leave the contribution of its citizens unnoticed, as they seemed to play a notable role in the defence of the nation in the first months of the full-scale war.

When comparing the civil activities in support of AFU with relevant U.S. and NATO documentation, similarities with resistance described in Resistance Operating Concept, as well 4 layers of national defence (individual, official, support to Home Guard and Asymmetric Defence Component) brought out in Comprehensive Defence Handbook stand out. Tasks for private sector described in the Comprehensive Defence Handbook (communications, transportation, supplying food and water, financial and material support, facilities, construction, cyber and medical assistance etc.) are strongly aligned with the support seen in Ukraine in the beginning of 2022 (NATO Special Operations Headquarters, 2020 pp. 58, 103; Senior officers of the Armed Forces of Ukraine, 2023). Therefore, it can be assessed that the special forces approach of involving civil population to support armed resistance has found use and confirmation of relevance in Ukraine during the full-scale invasion.

Based on the interviews with commanders of EDF and EDL, similar voluntary contribution of Estonian people as was seen in Ukraine is being counted on, and

preparations for accepting and utilizing it have been done for years. Ratings of readiness to utilize civil support differs between the commanders of EDF and EDL, however answers from both generals indicate that structure and understanding for utilizing civil support have been established.

Then again, commander of the EDF indicated to a gap in preparations that need to be completed in peace time to facilitate a quicker response by local companies for production of supplies needed for national defence. In case of an emerging threat, EDF active-duty officers will most likely be engaged in activities related to establishing the war time structure and procedures of the EDF, and the input for local companies is even harder to be composed then. Therefore, there seems to be a critical need for a systematic, e.g. project-based approach for preparing the necessary documentation, requirements, and guidance for local companies and population regarding their possibilities to contribute to Estonian defence in case of need. Knowledge about the preparations that need to be done prior to the war seem to exist in the EDF, however conducting the actual preparation seems to be the obstacle. Reasons for the obstacle need to be assessed separately.

A strong deficiency mentioned by General Ühtegi is the legislation that does not give the EDL specific roles for war time, as well limits their actions and preparations also in peace time. Therefore, it seems that knowledge and will for increase of capabilities exist, while laws and regulations limit the organizations development.

Based on the interviews with General Herem and General Ühtegi, it seemed that one of the biggest strengths for Estonian defence is the connection between the military and the society. Estonian Defence Forces train its reserves through conscription and therefore annually bring national defence closer to families of about 4 000 conscripts. Having nearly 50 000 active reservists and members of EDL as part of civil society enables strong connections and knowledge in different sectors and fields. Therefore, in peace time members of EDF and EDL carry their military mentality to their civil life and, in case of war, bring their civil expertise and connections to the military.

Overall, it can be assessed that the comprehensive approach to national defence creates supporting conditions for defending the country both with military and civilian means. However, to incorporate the support in a timely manner, EDF and EDL need

to contribute and prepare in peace time to reduce limitations and fill the gaps in their preparations.

Recommendations

Based on the analysis of the findings, recommendations can be made to increase the readiness of EDF and EDL:

- 1) Systematic and planned preparations should be carried out in the organization (EDF), possibly in cooperation with local companies, universities, or other parties, to prepare necessary plans and inputs for involving civil support to national defence.
- 2) Digital platforms that will become needed, and are in use in Ukraine, should be prepared and launched in peace time in cooperation with local experts, universities, or others.
- 3) Legislation should be assessed and adjusted to fully utilize the potential of EDL.

Solving of the matters mentioned above would provide a strong qualitative leap in the comprehensive approach to defence of Estonia.

Conclusion

Based on this research it can be assessed that for a small state such as Estonia, nation-wide comprehensive defence model is essential. Furthermore, the war in Ukraine has proven that in addition to official armed forces and defence structures, support from the society and population is vital, especially in the beginning of the war. The research conducted for writing this report was aimed at, and succeeded in, answering the following questions:

- Is resistance by civil population relevant in case of an intrusion by a foreign military?
- To what extent has the Estonian defence sector (Estonian Defence Forces, Estonian Defence League) prepared to accept and involve unorganized voluntary assistance to armed resistance based on examples from Ukraine from February to April 2022?

It is possible to assess that resistance by civilians is relevant in case of an intrusion by a foreign military because it enables rapidly responding to the threat. Additionally, widespread resistance and support to national defence mitigate capability gaps of official defence structures and provide additional, often specialized labour.

As for developing the Estonian defence capabilities based on experience from Ukraine, it seems that EDF and EDL have identified a vast number of lessons, however implementing the lessons into change still requires time and work. Estonia is preparing for involving public support to national defence via territorial defence units and on the grassroot level, making it less centralized and therefore flexible. Yet, steps the EDF must make themselves for involvement of civil support are not yet fully planned and prepared. Therefore, the readiness for institutional cooperation between the EDF and private sector need to be developed further.

Although there are plenty of lessons to learn from Ukraine and the commanders of EDF and EDL indicated that the learning process has not been effective enough, it seems that notable steps have already been taken and a couple of focused projects could significantly improve the results of implementing experience from Ukraine.

Bibliography

Brown, David. 2022. Ukraine conflict: Where are Russia's troops? *British Broadcasting Corporation*. 23 February 2022.

Eesti Uuringukeskus OÜ. 2023. Public opinion on national defence 2023. *Ministry of Defence*. [Online] July 2023. [Cited: 18 September 2023.] https://www.kaitseministeerium.ee/sites/default/files/public_opininon_and_national_defence_2023_spring.pdf.pdf.

Estonian Defence Forces. 2023. Estonian Defence Forces. [Online] 13 September 2023. [Cited: 18 September 2023.] <https://mil.ee/en/defence-forces/>.

—. **2023.** Maakaitse [Territorial Defence]. *Estonian Defence Forces*. [Online] 18 September 2023. [Cited: 17 October 2023.] <https://mil.ee/reserv/maakaitse/>.

Estonian Defence League. 2023. Estonian Defence League. [Online] Estonian Defence League, 17 October 2023. [Cited: 17 October 2023.] <https://www.kaitseliit.ee/en/edl>.

Estonian Foreign Intelligence Service. 2023. *International Security and Estonia 2023*. Tallinn : Estonian Foreign Intelligence Service, 2023.

—. **2024.** *International Security and Estonia, 2024*. Tallinn : Estonian Foreign Intelligence Service, 2024. p. 17.

Estonian Ministry of Defence. 2015. Initial self-defence capability and service in the military. *Estonian Ministry of Defence*. [Online] 13 August 2015. [Cited: 18 September 2023.] <https://www.kaitseministeerium.ee/en/objectives-activities/initial-self-defence-capability-and-service-military>.

—. **2018.** Leadership of the national defence. *Estonian Ministry of Defence*. [Online] 16 January 2018. [Cited: 18 September 2023.] <https://www.kaitseministeerium.ee/en/objectives-activities/leadership-national-defence>.

—. **2023.** National Defence and Society. *Estonian Ministry of Defence*. [Online] 21 July 2023. [Cited: 18 September 2023.] <https://www.kaitseministeerium.ee/en/objectives-activities/national-defence-and-society>.

Fiala, Otto C., Löfberg, Anders and Smith, Kirk. 2020. *Resistance Operating Concept*. MacDill AFB : Joint Special Operations University, 2020. ISBN 978-1-941715-43-7.

General Staff of Armed Forces of Ukraine. 2022. *Instructions for using Molotov cocktails*. Kyiv : X (Twitter), 28 February 2022.

Government of Estonia. 2023. National Security Concept of Estonia. *Ministry of Defence*. [Online] 23 February 2023. [Cited: 18 September 2023.] https://www.kaitseministeerium.ee/sites/default/files/eesti_julgeolekupoliitika_alused_eng_22.02.2023.pdf.

Herem, Martin. 2023. Commander of Estonian Defence Forces. [interv.] Taavi Karotamm. *Readiness to utilize civil support as seen in Ukraine*. Tallinn, 24 November 2023.

Keiley-Listermann, Meg, Lauber, Sam and Martin, Christine. 2019. *Resistance manual (draft)*. Fort Bragg : U.S. Army Special Operations Command, 2019.

Military Intelligence Center, Estonian Defence Forces. 2023. *Overview of the situation in Ukraine*. Tallinn : Estonian Defence Forces, 2023.

—. **2021.** Security Policy developments in Russia in 2021. *Annual Yearbook of Estonian Defence Forces*. 2021.

NATO Special Operations Headquarters. 2020. *Comprehensive Defence Handbook (Edition A ver. 1)*. SHAPE : NATO Special Operations Headquarters, 2020.

NATO Standardization Agency. 2013. *AAP-6 NATO Glossary and Terms (English and French)*. Brussels : NATO Standardization Agency, 2013. AAP-6.

Parliament of Estonia. 1992. Constitution of the Republic of Estonia. *Riigiteataja*. Tallinn : Parliament of Estonia, 1992.

—. **2023.** Estonian Defence Forces Organisation Act. *Riigiteataja*. Tallinn : Parliament of Estonia, 2023.

Senior officers of the Armed Forces of Ukraine. 2023. Civilian support to Armed Forces of Ukraine February-April 2022. Tartu : Baltic Defence College, 29 08 2023.

Sheth, Sonam. 2022. Ordinary Ukrainian citizens are taking up arms to fend off Russian forces as they close in on Kyiv. *Business Insider*. 25 02 2022.

Special Operations Force of Ukraine. 2022. *Civil resistance in occupied territories*. s.l. : Special Operations Force of Ukraine, 2022.

Stoltenberg, Jens. 2022. NATO Secretary General Jens Stoltenberg following an extraordinary meeting of the North Atlantic Council. *Press briefing*. s.l. : NATO, 24 February 2022.

U.S. Department of Defence. 2016. *Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms*. Washington D.C. : U.S. Department of Defence, 2016.

—. **2014.** *Joint Publication 3-05 Special Operations*. Washington D.C. : U.S. Department of Defence, 2014.

Wasielewski, Philip G. and Jonesand, Seth G. 2022. *Russia's possible invasion of Ukraine*. s.l. : Center for Strategic & International Studies, 2022.

Ühtegi, Riho. 2023a. Commander of Estonian Defence League. [interv.] Taavi Karotamm. *Readiness to utilize civil support as seen in Ukraine*. Tallinn, 24 November 2023a.

— . 2023b. Kaitseliidu arendamine ja riigikaitse lai käsitus [Development of Estonian Defence League and comprehensive approach to national defence]. *Kaitse Kodu!* August 2023b, pp. 5-6, 30. Extra section: 'Kaitseliidu sihtüksused: riigikaitse laia käsitluse toetuseks' ['Task units of Estonian Defence League: in support of the comprehensive approach to national defence'].

FELIX KESSERWAN. Equal Opportunity in the Armed Forces: A Case for Meritocratic Reforms

Introduction

Throughout history, militaries have been at the forefront of innovation; aiming at gaining an edge on potential foes and ensuring readiness to deal with new threats as they arise. While nomenclature, hierarchies, and ranks structures may have differed throughout time, from the Roman Legionaries to the French Foreign Legion, armies have been led by officers. Consequently, these leaders were in large part responsible for organizational changes, cultural transformations, and evolutions in tactics throughout the centuries.

It is well understood that armed forces are complex institutions that operate in a fragile balance between the need to maintain traditions, and the necessity to innovate. In the modern context, a question therefore emerges: how can military organizations change? While answers to this question may vary upon looking at the strategic, operational, or tactical levels; the role of leaders in enacting change is second to none.

This research paper will argue that military organizations must dismantle the remaining entrenched practices that undermine meritocracy, and reform the selection and development processes of its officer class to remain effective as a fighting force.

While this analysis applies to modern militaries as a whole, this paper will focus on the historical setting surrounding the officer class, the British reforms of the first and second world wars, the admission of women in military academies and Professional Military Education systems, and the common threads of officer development programs within NATO nations.

The first chapter will look at the historical evolution of the concept of military officers, focusing on requirements and illegibility criteria. The second chapter reviews the British departure from tradition during the first and second world war, granting temporary commissions to individuals that were not considered gentlemen in that historical

context. The third chapter will analyse the impact of women that have entered the officer corps of western militaries in the early 1980 and their contributions at the operational levels. Finally, the fourth chapter examines the remaining artificial barriers to the selection and development of officers in modern militaries, offering recommendations for change and reform.

The core of this paper focuses on meritocracy and its merits as a direct opposition to nepotism, discrimination, or simply arbitrary bias on which barriers to entry are built. For the purpose of this research, the concept of meritocracy should be understood as the evaluation of personnel and the setting of selection criteria based on competence, achievement, and capabilities, rather than social status, gender, personal connections, or any other external factors unrelated to the duties being performed.

Historical Setting

Implementing change in the military is notoriously slow; not only due to its tendency of being a large and complex organization, but because getting things wrong translates to lives lost. Therefore, military organizations remain on the conservative side, favoring practices that are time and battle proven and generally weary of novel ideas.

One of such practices is the separation of personnel between the enlisted and officer classes. This segregation can be traced back to the Roman Empire with the bulk of the soldiers being comprised from a mix of conscription and voluntary enlistment (Southern, 2007). In contrast, the Equites or the cavalrymen, along side the Senatorial class of Roman military leaders were recruited from the ranks of Patricians which constituted the Roman aristocracy (Talbert, 1996). Although the common soldier could potentially rise through the ranks after decades of demonstrating military skill, leadership, and prowess on the battlefield, the high-born were given command and leadership appointments right away (Duncan-Jones, 2016).

The first challenge to these entrenched practices and an attempt at organizational change was spearheaded by Gaius Marius, a Roman general and statesman, through what are known as the Marian reforms (Gauthier, 2019). These reforms were a series of changes that included the removal of the requirement to own land to become a Legionnaire, which greatly increased the number of eligible candidates (Beard, 2015).

It is important to note that these changes came at a time of crisis, fuelled by a need to bolster the ranks with more men for the North African campaign, and not an application of meritocracy (Duncan, 2017). Although a step in the right direction, the selection process for officers and commanders in the Roman military remained highly entrenched in tradition creating clear disparities in opportunities to lead.

The Marian Reforms fundamentally transformed the Roman military, making it a more formidable and effective fighting force. By allowing landless citizens to enlist, Gaius Marius significantly expanded the army's recruitment base, enabling Rome to field larger and more reliable armies. This professionalization of the military, along with improved organizational structures and standardized equipment, enhanced the Roman legions' operational effectiveness. Consequently, these reforms contributed to Rome's expanded influence and dominance over its adversaries, solidifying its status as a leading military power in the ancient world.

However, underlying concepts that helped rationalize the selection of officers from prominent families not die with the Roman Empire. Those that traditionally came from more affluent backgrounds received better education and were therefore considered to have the necessary qualities, discipline, and leadership skills to command men and respect. While the virtues of honor and loyalty to the state may have eroded over time, the emphasis placed on education above proven military proficiency still resonated centuries later; the term Patricians was simply replaced by Gentlemen.

British Departure from Tradition

From the end of the Napoleonic Wars, the British Empire emerged as a global power, built on the strength of its Navy which was unrivaled at sea, and its network of colonies spanning multiple continents (Spiers, 1992). At that time, the British Army stood apart from most of its rivals having developed a professional fighting force with built on experience gained from various conflicts and colonial wars (Leonhard, 2007). Additionally, beyond innovative military tactics and technologies, much of the army's success stemmed from effective command and control, enabled by a highly effective officer corps forged on lessons learned from around the globe.

While the British military had become a true institution by maintaining standing forces, the opening of military academies such as Sandhurst for Army officers, and Greenwich for Naval officers, its professionalized officer training still failed to incorporate meritocracy as part of recruitment (Otley, 1973). Until the late 19th century, officer commissions were to be purchased, allowing entry to the corps to only those with substantial means (Farwell, 1981). The existing training system, although effective in developing leaders, did not provide equal opportunity for joining, nor did it recognize military acumen among the enlisted men by appointing them to important command positions.

This practice was rationalized by several arguments: it primarily served as a safeguard against abuses of authority and gross negligence, ensuring that those commissioned acted properly, else they would be stripped of their commission without financial compensation (Bruce, 1980). Additionally, this approach maintained a social and political status quo, ensuring that the officer class was comprised of actors loyal to the crown, reducing the risk of internal rebellions or coups (Bruce, 1980). In 1871, under the leadership of the Secretary of State for War Edward Cardwell, the practice of purchasing commissions was finally abolished as part of the Cardwell reforms, a very controversial decision at the time (Tucker, 1963).

Although significant, the Cardwell reforms did not change the fact that until World War I, the British officer corps was still comprised of individuals from privileged backgrounds with the exception of those in the artillery and engineer corps (Southern, 2007). For the most part, these men came from affluent families who saw the military as a pathway to increase their social status and in some cases, help launch their political careers: these individuals were often referred to as 'gentlemen officers'. It is also important to note, that contrarily to the common soldier, officer positions were relatively safe, with codes of honor still in place which discouraged the direct targeting of officers on the battlefield (Gates, 2001).

This reality would come to change at the turn of the 20th century and the eruption of World War I. With significant advancements in both armament and tactics, the scale of destruction and death during the four-year conflict was unmatched. Officers were also not immune from this reality, recording significant losses, especially in the early years of the conflict. The unprecedented losses combined with the sheer scale of the conflict

forced the British empire to depart from tradition and appoint what would be later known as 'Temporary Gentlemen' (Deeks, 2017).

The Great War did not discriminate between officers and non-commissioned members ravaging through trenches at a scale of thousands of dead per day (Office, 1922). Victorian-era ideals that formed the basis of the gentleman-officer class which included social behavioral expectation, class distinction, decorum, manners, and adherence to social conventions were supplanted by more pragmatic attributes. It was once again crisis and the challenging conditions of the battlefield that triggered a call for change, leading to a reassessment of traditional norms.

Contrarily to previous conflicts, officers were often in the thick of the fighting, exposed to the same dangers as their enlisted counterparts. The realities of war necessitated a reassessment of what makes an effective officer and leader in opposition to a strict adherence to a traditional gentlemanly conduct (Deeks, 2017). Officers were called to command troops comprised in large part of conscripts in a highly challenging and deadly environment, further complicating their role. The act of leading men in battle became a privilege reserved for those that demonstrated the proper tactical acumen and the ability to maintain composure under fire.

This shift away from social niceties to an emphasis on meritocracy, military effectiveness, and leadership qualities, did not mark an abandonment of professionalism or discipline, but rather acknowledged the realities of the wartime context (Deeks, 2017). Enabled by a dedication to the welfare of the troops and unwavering commitment to achieving victory at any cost, that meritocracy took center stage judging officers by their ability to lead and make sound tactical and operational decision rather than conforming to social expectations.

To further exemplify this shift towards meritocracy, it is important to note that many of the soldiers that were granted temporary commissions came from the ranks, transitioning from non-commissioned officer (NCO) positions and assuming command as officers (Holmes, 2011). Those NCOs that demonstrated strategic expertise and leadership qualities under the realities of warfare were quickly identified and granted the privilege to lead. Although in some cases the transition from Regimental Sergeant Major, holding authority over hundred of men, to the position of second lieutenant was

difficult, it was nevertheless a promotion; the ability to make decisions rather than merely advising (Holmes, 2011).

The success of this reform cannot be understated as it not only had effects from a tactical and operational front, but also positively affect moral and discipline. In regard to morale, battle proven NCOs commanded the respect of the troops even when being posted away from their units, which was a practice meant to ensure that officers were not too familiar with their men. As for discipline, those that transitioned from the ranks had a distinct advantage over their direct entry counterparts: 'subject to hostility from their men for knowing too much of army life and being difficult to fool compared to traditional officers' (Holmes, 2011).

Although the experiment had been successful by all relevant metrics, leading to Entente Powers' victory in 1918, the post WWI era was marked by extensive demobilisation. The temporary gentleman status was abolished and by the end of 1920 most of the officers holding temporary commissions were dismissed (Petter, 1994). It appeared that once the crisis had passed, calls for a return to normalcy overshadowed the progress and successes achieved during the Great War: *status quo ante bellum*. In the words of John Turner: 'the army was at work scraping off the reality of war and burnishing up the war-tarnished conventionalities of peace' (Turner, 2014). The reality was such that the end of the war saw the return of expensive social habits for officers which excluded those of lesser means that simply couldn't maintain their positions in the peacetime army (Holmes, 2011).

Nearly twenty years later, the British military found itself in a familiar position at the onset of World War II: a shortage of officers and an enemy at the gates. With only fourteen thousand officers in the regular force and nineteen thousand in the territorial army, the United-Kingdom introduced the National Service Act of 1939. While the initiative succeeded in bolstering the ranks, awarding commissions to nearly two hundred and fifty thousand men, their integration into a cadre reserved for the upper classes was difficult to say the least (Holmes, 2011). Compounding the issue, these newly commissioned officers, for the most part, lacked prior military experience and were thrust into a conflict that saw the incorporation of the air domain and a significant increase of pace on the battlefield with the advent of highly mobile mechanised units. This was yet another testament that organizational change is

typically triggered by moments of crisis but should instead be developed during peace time.

Recognizing the need for a deliberate approach to the selection and development of officers the United Kingdom introduced the War Office Selection Board (WOSB) in April 1942. This significant change was the result of reforms that began in 1941 with the introduction of Command Interview Boards, and calls from the Labour to reform the system: 'the present Army system ... under which officer commissions are almost wholly reserved for the sons of the well-to-do is out of date in a democratic country' (UK Parliament, 1938). This novel approach marked an important departure from conventional practices which would not be overturned even after the war. Although recruitment from the lower classes to the officer corps did not initially increase due to the fact that merely six per cent of candidates conscripted were deemed suitable, the process was set and would be fair and transparent going forward (Holmes, 2011).

In 1945 once the victory by the Allies was secured, the British government entered a transition period, making sure not to repeat the mistakes committed post World War I. A large and sudden demobilization did not take place, but instead saw temporary officers being utilized to meet the ongoing military and reconstruction needs at home and abroad (Allport, 2010). Furthermore, the end of the most destructive conflict on European soil also marked a cultural shift in the British society, breaking down many of the class related stigmas which began to diversify the labour force in many domains, including the military (Allport, 2010). Less than two decades later, the term 'temporary gentlemen' fell out of use, and by the 1970s was officially removed from military terminology reflecting a shift in perceptions and priorities (Mileham, 2004).

As for the impact of this change, suspending the requirement for officers to come from the 'gentleman' class during WWI and WWII had a profound impact on the British military, making it a more effective fighting force. This democratization allowed for the promotion of individuals based on merit and capability rather than social class, broadening the talent pool and ensuring that leadership positions could be filled by those with proven skills and leadership qualities. This shift not only improved military efficiency and adaptability but also reflected broader social changes towards meritocracy and inclusivity.

In summary, it is clear that institutional changes in the military can take decades to trial and implement, especially when they are rooted in societal norms and traditions. Furthermore, the common denominator between attempts at reforms during the first and second World War are times of crisis and military necessity: alternative ideas and approaches are explored in times where the status quo is proven ineffective. Unfortunately, as it is often the case, the end of a crisis also calls for a restoration of traditions, overlooking the progresses made during that time. The British departure from tradition at the turn of the 20th century and once again during the second World War, are concrete examples of successful transformations to the way an armed force can recruit and develop its officers; removing barriers to entry and assessing candidates on objective metrics and dispositions. However, while the War Office Selection Board helped break down entrenched practices as they relate to class, it did nothing to integrate women into the officer class, an endeavour that would take multiple decades to be achieved.

Integration of Women in Officer Corps

The integration of women into the officer corps and more broadly the military, can be traced back to the Second World War. While there is no debate that women assumed military leadership roles prior to 1939, World War II marked a significant shift in gender roles particularly in the West which was embroiled in conflict (Carreiras, 2004). During that time, women served in a various capacities, primarily in administrative roles, but also in the medical field, communications, code-breaking, anti-aircraft units, and even aviation.

While the struggle of men to join the officer class in the 20th century was primarily rooted in class warfare, the women faced an uphill battle built on centuries of stereotypes and pre-conceived ideas. From 1945 onward, the inclusion of women in the officer corps of Western nations has been a significant development for their armed forces (Campbell, 1993). Historically, women were excluded from combat roles and high-ranking officer positions, limiting their contribution to rear echelon and secondary roles. The perception of women's combat abilities and roles in the military changed during the Second World War (Campbell, 1993).

Several women contributed to the breaking of barriers during that time. Jacqueline Cochran was a pioneer aviator that led the Women Airforce Service Pilots (WASP) program enabling women to assume the roles of pilot in the United-States. Dame Vera Laughton Mathews as director of the Women's Royal Naval Service (WRNS) played a pivotal role in the integration of women into the British Royal Navy (UK National Archives, 1954). Canadian Elsie MacGill though not a military officer, provided significant contributions to the production of aircraft for the Royal Canadian Air Force, trailblazing the entry of women in military STEM (Bourgeois-Doyle, 2008). Major Lyudmila Pavlichenko born in Ukraine served the Soviet Union as a sniper demonstrating female abilities in combat totalling 309 confirmed kills (Pegler, 2018).

Despite these contributions and achievements, the end of the Second World War saw most women leave or being pushed out of the military, returning to their traditional societal roles. Those that remained in the force were denied equal opportunity for advancement and faced significant challenges and gender-based barriers (Campbell, 1984). It would take over three decades for Western policy makers to take decisive action in integrating women into the officer class. The United States were among the first to ratify official policy allowing women to be admitted to military academies, which saw the first 119 women joining the Corps of Cadets of Westpoint on July 7, 1976 (Henry, 2006). Four years later, Canada followed suite by opening the doors of the Royal Military College to thirty-two women in 1980 (Armstrong, 2019). Similarly, in 1984, the British Women's Officer Training College Bagshot was merged with the Sandhurst Academy insuring both men and women receive the same officer training going forward (National Army Museum, 2024).

While the political framework for the integration of women as leaders in the military was in place at the highest echelon, the realities in line units were starkly different. Katherine Baggaley writes: 'a woman's succession into the military masculine culture depends on her ability to physically appear, communicate, and behave as a man' (Baggaley, 2019). Female officers that disturbed the status quo experienced significant backlash which impacted their career progression. The realities of women being held back and passed for promotions became so prevalent that new policies had to be passed as an attempt to address this discriminatory phenomenon: in Canada, the Pink List or Pink Seat policy added a requirement for a quota of positions to be held by

women, especially on Command and Staff Courses which are prerequisites for promotion (Davis, 2007).

These examples serve to show that organizational change in institutions such as the military must trickle down from the politico-strategic, to the operational and tactical realm encountering resistance and pushback at each stratum. Focusing on the positive, it is undeniable that the inclusion of women into the officer corps of Western militaries has had numerous positive effects at the operational level. The three most enduring examples are the expansion of the recruiting talent pool, operational effectiveness, and the integration of diverse skills and perspectives in the decision-making process.

First, as it related to expanding the talent pool, female officers fill a crucial role in specialized fields that require high levels of education and expertise as they now represent over half of the individuals holding tertiary degrees in the West. Additionally, in sectors such as medicine, engineering, cybersecurity, and intelligence, where the military competes with the private sector, 'women's inclusion not only broadens the pool of potential recruits but also helps to fill critical capability gaps' (Service, 2017).

Second, in terms of operational effectiveness, recent conflicts in Afghanistan and Iraq have shown that the participation of women in both combat and peacekeeping roles enhances information and intelligence gathering operations: 'In environments where cultural norms restrict interactions between women and men from outside their community, female soldiers can access populations and gather intelligence that would be off-limits to their male counterparts' (United Nations, 2017). This capability extends to CIMIC operations and other aspects such as delivering effective humanitarian aid and support, while building trust within the communities engaged.

Third, it is important to emphasize the contribution of women to the armed forces in terms of the diverse skill sets and perspectives they provide. By bringing different experiences and viewpoints to the decision-making process, female officers assist in developing a more holistic approach to both problem-solving and operational planning. In a report published in 2015, the consulting firm McKinsey highlighted the impact of diversity in the private sector: 'Research has shown that mixed-gender teams often outperform single-gender teams in problem-solving tasks due to the diversity of

perspectives and approaches' (McKinsey & Comapny, 2015). In the military context, these contributions translate to novel ways of tackling existing problems, the development of new strategies to conflict resolution, and engagement with a broader range of stakeholders. Similarly, at the operational level, female involvement helps leaders develop a more encompassing situational picture and a better understanding of the complex social and cultural landscape in which armed forces operate.

To summarize, the inclusion of women into modern armed forces as part of the officer class, marked an important shift toward gender inclusion in Western militaries. The process is still ongoing, evident by the breaking down of artificial barriers, notable achievements, and enduring challenges. Since the end of the Second World War, female roles in the Armed Forces have evolved from specialized support to taking active roles as leaders, involved in the decision-making process. Female integration has shown to be a net positive on the entire spectrum of operations, from combat to peacekeeping, helping build more capable and adaptable units, contributing to mission success.

Remaining Barriers

The thirty-two NATO nations forming the alliance today represent great strides in building professional and inclusive armed forces. Although we are far removed from the times when land ownership, class or gender had an incidence on one's eligibility to become an officer, artificial barriers remain that prevent a truly meritocratic approach to officer selection and development in the West (Linn, 2008). Although each of the NATO nations have differences in their military recruitment, retention, and professional development processes, commonalities emerge (Nikolić, 2009). The three key commonalities are prerequisites that are not directly linked to employment, a one-size-fits-all approach to professional education, and an outdated approach to the filling of vacancies.

In terms of prerequisites that are not linked to employment, the two mains are the requirement for advanced education, and arbitrary physical fitness standards. The term advanced education refers to post-secondary schooling which in most cases refers to a first cycle university degree (Forsling, 2017). It important to note that although there are exceptions to the rule (promotion from the ranks, technical equivalencies, etc.) a

college degree is a common requirement for commissioned officers in most NATO countries.

Professor of Behavioral Sciences at the U.S. Army War College, Colonel (Retired) Stephen J. Gerras, Ph.D. writes that this requirement 'is based on the belief that higher education provides essential leadership, critical thinking, and management skills, although the direct applicability of the degree to military duties varies' (Gerras, 2008). I would argue that this rationale is faulty and lacks objective metrics; it is reminiscent of the class-based ideals of the Victorian-era. Furthermore, it is important to note that at the height of the Second World War less than 5% of Americans and Europeans had four years of college: this number has climbed to over 40% today.

The requirement for a university degree represents a barrier to entry for those with lesser means and does not adequately screen candidates against objective factors or job requirements. In an increasingly competitive labour market, leading firms Google, IBM, Tesla, and Accenture have eliminated such requirements to attract the right talent (Caminiti, 2022). These industry leaders focus on evaluating candidates solely based on their competency, utilizing a blend of technical assessments and personality test to identify key qualities such as leadership, critical thinking, and management skills.

As for fitness standards, there is no argument that the military is a physically demanding career which requires a certain level of endurance. However, the applications of such standards in the military tends to be arbitrary and adopt a blanket approach to an organization with a variety of employment (Lewis, 1999). Many NATO countries still maintain gender-specific physical fitness standards, setting different minimum requirements based on gender. Furthermore, in most cases these standards are applied notwithstanding of occupation; infantry soldiers and administrative clerks being held to the same minimal requirement (Lewis, 1999). These practices turn away viable and motivated candidates, who's physical fitness can undoubtedly be developed once in the service.

Similarly, a standardized approach to professional military education fails to identify and develop those officers outside the core function of combat and combat support (Neumann, et al., 1989). A study of officer development programs among NATO allies has found that in Canada, France, Germany, Great Britain and the United States, an

officer will spend on average three years between the ranks of second lieutenant and lieutenant-colonel in the military education system (Linn, 2008).

While course names may differ from one nation to another, there are some stark similarities: the courses are pre-requisites for promotion, the selection process is ambiguous, and the curricula focuses on developing staff skills and general operational acumen (Caforio, 2018). Although this approach may be adequate to meet the basic aim of military education it fails on two fronts: the selection candidates based on merit, and the development of technical experts in their respective fields.

Regarding the aspect of meritocracy in the selection process of candidates, it is understood that each military conducts some sort of succession planning that leads to the selection of candidates to be sent on these courses. With that said, in opposition to counterparts in the public and private sectors, these boards are not open nor transparent, relying heavily on seniority, and subjective appraisals (Wilcove, et al., 1990). Furthermore, although there are exceptions, professional military education establishments are not conducting their own screening or assessment of candidates upon entry, but rather rely on the recommendations of respective chain of commands; this practice further exacerbates the echo chamber effect in the selection and development of future leaders.

Likewise, the current officer development programs tend to overlook the needs of keeping technical experts current in their respective domains, prioritizing the transmission of a common core curriculum aimed primarily at combat and combat support personnel (Neumann, et al., 1989). With the amount of time spent developing staffing skills and intercomponent interoperability, an opportunity is missed to recognize and develop those in the more technical fields that would benefit from collaboration and education amongst industry leaders. This particular barrier is one of mindset; large organizations tend to prioritize a one-size fits all approach to talent development and career progression, rather than developing more fluid pathways to promotion.

Moreover, the process by which the military fills its vacancies is yet another example of an outdated approach and a system that has not been updated in decades. While on the surface Western militaries have enacted policies that encourage inclusion and

diversity in recruitment, staffing, and promotion practices, the process by which officers are appointed to fill vacancies is neither fair nor transparent. For the most part, civilian organizations take the time to advertise vacancies, outline position requirements and pre-requisites, list essential and desirable qualifications, and hold standardized selection boards to choose the right candidate(s). In contrast, military organizations rely on closed door discussions centered around the subjective appraisals of eligible candidates (Wilcove, et al., 1990).

The consequence of these practices is a diminished sense of control officers have over their careers, reportedly contributing to decisions of leaving the military, which adversely impacts retention rates (Filosa, 2020). The lack of transparency, combined with an unclear and opaque decision-making process as it relates to promotions and assignments leads to disillusionment among capable and motivated officers. Adhering to the basic principles of meritocracy, where promotions and opportunities are based on clear and fair criteria, would enhance officers' sense of control over their careers, potentially improving retention by aligning military processes with modern expectations of fairness and inclusivity.

In conclusion, dismantling the remaining barriers amongst the armed forces comprising NATO, is a necessary step to enhance the alliance's effectiveness as a fighting force. The above-mentioned entrenched practices that oppose merit-based approaches to the selection and development of officers not only undermine ideals of diversity and inclusion, but also impact organizational adaptability and operational readiness. By adopting transparent, fair, and competency-based criteria for selection, militaries would implement private industry best practices leveraging the talent of their personnel, and in turn fostering a dynamic, capable, and resilient force prepared to face the challenges of modern warfare.

Conclusion

In conclusion, having analysed the evolution of officer development and progression from a historical class-based perspective, and examined implication of the modern inclusion of women in Western military officer corps, it is clear that the dismantlement of entrenched practices that undermine meritocracy contributes to building more effective militaries. While much progress has been made, and important milestones have been reached, the ongoing recruiting and retention issues underscore the necessity of implementing the above-mentioned proposed reforms. To this day, barriers that impede the full realization of a merit-based approach to officer selection and career progression remain in place withing NATO militaries. In terms of policy recommendations, this paper stands to highlight the importance of revisiting outdated prerequisites, such as advanced education requirements and physical fitness standards, not as criteria, but as a one size fits all approach to career progression. By implementing private sector proven best practices, militaries will better align with the contemporary needs of their organizations and attract a wider pool of qualified candidates. Placing meritocracy as a cornerstone of military culture would enhance operational effectiveness, adaptability, and readiness for future challenges.

Bibliography

Allport, Alan. 2010. *Demobbed: Coming Home After the Second World War*, New Haven. New Haven : Yale University Press, 2010. Vol. 83. ISBN: 9780300168860.

Armstrong, Kate. 2019. *The Stone Frigate: The Royal Military College's First Female Cadet Speaks Out*. Kingston : Dundurn Press, 2019. ISBN: 978-1459744059.

Baggaley, Katherine. 2019. The progressions of a gendered military: A theoretical examination of gender inequality in the Canadian military. *Journal of Military, Veteran and Family Health*. First, 2019, Vol. 5, 1.

Beard, Mary. 2015. *SPQR: a history of ancient Rome*. New York : Liveright Publishing Corporation, 2015. ISBN 978-0-6556-4914-4.

Bourgeois-Doyle, Richard I. 2008. *Her Daughter the Engineer: The Life of Elsie Gregory MacGill*. Ottawa : NRC Research Press, 2008. ISBN 978-0-660-19813-2..

Bruce, Anthony P. C. 1980. *The Purchase System in the British Army*. London : Royal Historical Society, 1980. Vols. Family Tree Magazine, vol. 23, no. 7, pp. 10–13. ISBN: 0901050571.

Caforio, G. 2018. Military Officer Education. *Handbooks of Sociology and Social Research*. 1, 2018, Vol. 22, 3.

Caminiti, Susan. 2022. No college degree? No problem. More companies are eliminating requirements to attract the workers they need. *CNBC*. [Online] CNBC, April 27, 2022. [Cited: March 17, 2024.] <https://www.cnbc.com/2022/04/25/companies-eliminate-college-degree-requirement-to-draw-needed-workers.html>.

Campbell, D'Ann. 1984. *Women at War with America: Private Lives in a Patriotic Era*. Cambridge : Harvard University Press, 1984. ISBN: 978-0674954755.

—. 1993. Women in Combat: The World War II Experience in the United States, Great Britain, Germany, and the Soviet Union. *The Journal of Military History*. First, 1993, Vol. 57, 2.

Carreiras, Helena. 2004. *Gender and the Military: Women in the Armed Forces of Western Democracies*. New York : Carocci, 2004. ISBN: 9780203969038.

Davis, Karen D. 2007. *WOMEN AND LEADERSHIP IN THE CANADIAN FORCES: PERSPECTIVES AND EXPERIENCE*. Kingston : Canadian Defence Academy Press, 2007. ISBN: 978-0-662-46296-5.

Deeks, Roger. 2017. *Officers Not Gentlemen: Officers Commissioned from the Ranks of the Pre-First World War British Regular Army, 1903–1918*. Birmingham : University of Birmingham, 2017.

Duncan, Mike. 2017. *The Storm Before the Storm: The Beginning of the End of the Roman Republic*. London : Public Affairs, 2017. ISBN: 978-1610397216.

Duncan-Jones, Richard. 2016. *Power and Privilege in Roman Society*. Cambridge : Cambridge University Press, 2016. ISBN: 9781316575475.

Farwell, Byron. 1981. *For Queen and Country: Social History of the Victorian and Edwardian Army*. London : VIKING, 1981. ISBN: 978-0713912418.

Filosa, Lorenzo. 2020. The Military Academic Motivation Scale (MAMS): A New Scale to Assess Motivation Among Military Cadets From a Self-Determination Theory. *European Journal of Psychological Assessment*. 1, 2020, Vol. 37, 3.

Forsling, Carl. 2017. It's 2017. The Military Still Requires Officers To Have College Degrees. Why? *Task & Purpose*. [Online] Task & Purpose, October 15, 2017. [Cited: March 17, 2024.] <https://taskandpurpose.com/news/2017-military-still-requires-officers-college-degrees/>.

Gates, David. 2001. *Warfare in the Nineteenth Century (European History in Perspective)*. London : Palgrave Macmillan, 2001. ISBN: 978-0333735343.

Gauthier, François. 2019. The transformation of the Roman army in the last decades of the Republic. *Romans at War*. Abingdon : Routledge, 2019.

Gerras, Stephen J. 2008. *THINKING CRITICALLY ABOUT CRITICAL THINKING: A FUNDAMENTAL GUIDE FOR STRATEGIC LEADERS*. Washington : U.S. Army War College, 2008.

Henry, Jacob M. 2006. *PRIDE AND EXCELLENCE: THE FIRST CLASS OF WOMEN AT WEST POINT*. [Web] Washington : National Museum, 2006.

Holmes, Richard. 2011. *Soldiers: Army Lives and Loyalties from Redcoats to Dusty Warriors*. New York : Harper Press, 2011. ISBN 978-0-007-22569-9.

Leonhard, Jörn. 2007. Nations in Arms and Imperial Defence – Continental Models, the British Empire and its Military before 1914. *Journal of Modern European History*. First, 2007, Vol. 5, 2.

Lewis, Jay S. 1999. *Military Officer Appraisal, An Examination*. Maxwell : AIR COMMAND AND STAFF COLL MAXWELL AFB AL, 1999. ADA395121 .

Linn, Major William D. 2008. *Officer Development: A Contemporary Roadmap* . Fort Leavenworth, Kansas : School of Advanced Military Studies United States Army Command and General Staff College , 2008.

Linn, William. 2008. *Officer Development: A Contemporary Roadmap*. Fort Leavenworth : ARMY COMMAND AND GENERAL STAFF COLLEGE, 2008. ADA485472.

McKinsey & Comapny. 2015. *Diversity Matters*. New York : McKinsey & Comapny, 2015.

Mileham, Patrick. 2004. Fifty Years of British Army Officership 1960–2010. *Defense & Security Analysis* . First, 2004, Vol. 20, 1.

National Army Museum. 2024. *Sandhurst, officers and the role of history*. [Web] London : s.n., 2024. 237902.

Neumann, Idell, Mattson, Joyce D. and Abrahams, Norman M. 1989. *Development and Evaluation of an Officer Potential Composite*. San Diego : NAVY PERSONNEL RESEARCH AND DEVELOPMENT CENTER, 1989. ADA213471.

Nikolić, Nebojša. 2009. Culture Of Career Development And Ranking And Selection Of Military Officers. *Western Balkans Security Observer - English Edition*. 2009, 14.

Office, Great Britain War. 1922. *The War Office, Statistics of the Military Effort of the British Empire During the Great War 1914–1920*. London : London: H.M. Stationery Office, 1922.

Otley, C. B. 1973. The Educational Background of British Army Officers. *Sociology*. First, 1973, Vol. 7, 2.

—. "*The Educational Background of British Army Officers*".

Pegler, Martin. 2018. *Lady Death: The Memoirs of Stalin's Sniper*. London : Greenhill Books, 2018. ISBN: 978-1784382704.

Petter, Martin. 1994. Temporary Gentlemen' in the Aftermath of the Great War: Rank, Status and the Ex-Officer Problem. *The Historical Journal*. First, 1994, Vol. 37, 1.

Service, Congressional Research. 2017. *Diversity, Inclusion, and Equal Opportunity in the Armed Services: Background and Issues for Congress*. Washington : CRS Report, 2017. R44321.

Southern, Pat. 2007. *The Roman Army: A Social and Institutional History*. Oxford : Oxford University Press, 2007. ISBN: 978-0195328783.

Spiers, Edward M. 1992. *The Late Victorian Army, 1868-1902*. Manchester : Manchester University Press, 1992. ISBN: 978-0-7190-2659-1.

Talbert, Richard J. A. 1996. The Senate and senatorial and equestrian posts. *The Cambridge Ancient History*. Second, 1996, Vol. 10.

Tucker, Albert V. 1963. Army and Society in England 1870-1900: A Reassessment of the Cardwell Reforms. *Journal of British Studies*. First, 1963, Vol. 2, 2.

Turner, John. 2014. *Britain and the First World War*. London : Routledge Library Editions, 2014. ISBN 9781317692140.

UK National Archives. 1954. Dame Vera Laughton Matthews to Mrs Horton. *The National Archives*. [Online] June 6, 1954. [Cited: February 28, 2024.] <https://discovery.nationalarchives.gov.uk/details/r/b523ee87-b034-4407-9632-c0b4407f6eae.9/01/1328>.

UK Parliament. 1938. *Army Estimates - Mr. Hore-Belisha Steatement*. London : UK Parliament, 1938.

United Nations. 2017. *Improving Security of United Nations Peacekeepers: We need to change the way we are doing business*. New York : United Nations Headquarters, 2017.

Wilcove, Gerry L., et al. 1990. *Officer Career Development: A Review of the Civilian and Military Research Literature on Turnover and Retention*. San Diego : NAVY PERSONNEL RESEARCH AND DEVELOPMENT CENTER, 1990. ADA241363.

IMANTS KLEINBERGS. Critical Infrastructure Protection System And Resilience in Latvia

Introduction

The Information era, where new technologies, new weapon systems, and Artificial Intelligence were applied in warfare, led us to the prospect that future wars will be based on precision strikes and the speed of joint effort and will last for a short time (Fridbertsson, 2022). The war of attrition stemmed from World War II, where both sides attacked each other and tried to influence critical national infrastructure, seemingly becoming absolute. Looking at the war in Ukraine, we can see that attrition warfare has not gone far away. New technology is enhancing old methods.

The war in Ukraine shows Russia's imminent threat towards critical infrastructure essential for civil society. Especially effective are attacks against critical national infrastructure that provides electricity or energy, thus influencing any other type of national critical infrastructure to disrupt vital civil society services (Harmash, Balmforth, 2023). Cheap Unmanned Aerial Vehicles, Tactical Ballistic Missiles and Cruise missiles cause damage to Critical National Infrastructure, including electricity substations, power plants and even infrastructure that supports nuclear stations. By damaging infrastructure providing energy, Russia is achieving its aim of disrupting other services for civil society that support Ukrainian Military Forces. There are signs that the military theory of Warden's rings has been used, which suggests eliminating the strategic centre of gravity - leadership, command and control elements and essential critical infrastructure (Cohen et al., 2020). Daily news is broadcasting attacks by Russia with drones and missiles. The Ukrainian side is claiming a significant percentage of those attacks have been countered by their air defence systems even though substantial numbers of drones and missiles slip through and cause damage. But if Ukraine did not have support from European countries and did not have a layered Air defence system in place, then losses and damage to infrastructure would have been worse. So, the lesson identified from the war in Ukraine is that to counter Russian threats by drones and missiles, there is a need to change the mindset about air defence and to rethink how to reconfigure air defence systems to effectively address emerging

threats to critical infrastructure. Latvia is a border country of NATO with Russia in the Eastern Flank, and all the threats should be taken seriously. Thus, critical national infrastructure should be Latvia's top priority. Passive defence methods, like hardening, cover and camouflage, should be used where possible.

Considering the lessons mentioned above identified from the war in Ukraine, this research will argue that the Critical National Infrastructure Protection system and resilience of infrastructure in Latvia are inadequate, particularly considering the lessons identified from the conflict in Ukraine due to a lack of comprehensive counter-drone measures and appropriate protection against long-range threats.

The first paragraph will address the current threat posed by drones, particularly as loitering munition, and examine Latvia's plans for developing a counter-unmanned aerial vehicle system. It will also discuss existing systems in Latvia capable of countering drones, including kinetic and electromagnetic solutions.

The second paragraph will focus on the long-range missile threat and Latvia's acquisition plans for a new air defence system, such as the German-made medium-range air defence system IRIS-T. It will analyse the system's application strategies and assess its potential effectiveness in countering long-range threats to critical infrastructure.

In conclusion, this research will recap the actuality of the topic. It will summarise the assessment of Latvia's capability to counter unmanned aerial vehicles and long-range missile threats. This research will come up with recommendations for developing additional air defence systems capable of countering threats from unmanned aerial vehicles and missiles and propose actions to establish security measures for the enhancement of the security situation.

1. Countering Unmanned Aerial Vehicles (Drone Threats) in the context of defending Critical Infrastructure.

1.1. Actuality of the threat.

According to Latvian Law about National Security, Critical National Infrastructure are objects, systems or parts thereof and services located in the Republic of Latvia which are essential for the implementation of important functions of society, as well as the protection of human health, safety, economic or social for the provision of welfare and the destruction or disruption of the activities of which would have a significant impact on the State and society implementation of basic functions (Saeima of Latvia, 2023). Critical National Infrastructure is essential for the existence of any developed country. Energy infrastructure, water systems and communication infrastructure are crucial utilities for the population. People are used to these utilities, which are essential for daily life and the existence of humans. At the same time, it is vulnerable to threats from drones.

Actuality and potential threats from drones lie in some key characteristics that make drones more available and favourable for warfighting. The first factor to address is the relatively low costs of drones and accessibility in the world's market. The most used Shahed 136 drone costs approximately 20,000 USD (BBC News, 2023). The development of technologies in the area of drones made them available around the world. Mass production of parts of the drones and demand from the civilian sector made the drones cheap and with unlimited access. Not only Western countries but also Middle Eastern countries, like Syria, have gained that technology and are producing their own drones. The second factor to address with the actuality of the threat from drones is automation. Programming of the routes and usage of artificial intelligence to seek targets made drones easy to utilise as an offensive weapon and, with relatively low cost, made the drones become a daily threat to Ukraine in its ongoing war with Russia.

Lastly, with the development of batteries and other components, drones have become lighter and capable of carrying a significant payload. Drones can carry different types of equipment and can be used to deliver vital resupplies to troops in danger, but most significantly, drones can carry explosives in the form of improvised explosive devices,

or drones can be rebuilt and adapted to kamikaze or loitering munition types of weapons.

1.2. How is Russia using UAVs to threaten Ukraine's Critical Infrastructure?

For non-specialists in the area, it was a common belief that drones were used more for Intelligence Surveillance Reconnaissance (ISR) purposes, and available statistics show that before the war in Ukraine, Russia developed mainly UAVs for troop assistance with ISR information and target acquisition. When Russia depleted its resources of ballistic missiles, they soon realised that UAVs could be used as cheaper weapons. Ukraine had to face a new challenge – defence against small UAVs used as loitering ammunition.

After massive attacks in the early stages of the war on 24 February 2022, Russia used many Cruise and Ballistic missiles, making attacks very expensive and hardly sustainable. There was a need for an alternative solution. This is where Shahed-136 came into play in the autumn of 2022. Russia started using Iranian-made Shahed-136 as a loitering munition to compensate for the shortage of cruise missiles. Shahed-136 is considered a loitering munition capable of carrying 50-60kg explosives in a distance of 1500-2000km (BBC News, 2023).

Russia uses this drone to overwhelm Ukraine's Air defence and attack cities and power stations. Shahed-136 is motor-pushed loitering ammunition with a wingspan of 2.5 meters. Considering the small size compared to aircraft, it was hard to detect it with radars by Ukraine (BBC News, 2023). At the initial stage of the war, Ukraine used old post-soviet radars that were not designed to detect UAVs.

Since this research is focused on critical infrastructure, Russian ISR drones are excluded from the assessment of threats, and the focus will be on methods of fighting “kamikaze” UAVs as loitering munition.

Russian strategy of using drones is the same as they would use the missiles. The strategy is to employ drones in bigger groups, ten to twenty or even thirty drones at a time, so the air defence systems of Ukraine are triggered and overwhelmed. Relatively

expensive air defence missiles from the launchers are fired, and with a kill ratio of around eighty per cent, four to five drones slip through and reach their targets. Follow-on action from the Russian side is to fire missiles to exploit gaps in the air defence bubble and penetrate targets with bigger explosive warheads. Until April of 2023, Russia has used 750 Shaheed drones with the same strategy (Hagen, 2023).

"The Ukrainian source said Russia is now able to assemble the Shahed-136 systems itself at a facility in the Tatarstan region, 500 miles east of Moscow. "The manufacturing capacity [by] September 2025 should be around 4,000 pieces per year," the source said." (Haynes, 2024) This information from the Skynews portal is alarming and delivers the message that the actuality of the threat from Shaheed drones will rise and will ask for great effort from Ukraine to counter it.

1.3. How do other countries attempt to protect Critical Infrastructure against the threat of UAVs, new trends and good practices?

There is no universal solution towards UAV threats like Shahed-136. Considering other threats like cruise missiles and aircraft threats, most Western militaries try to reach layered air defence capabilities with different radars and engagement sources, providing sophisticated Command and Control options for decision-makers to choose the best weapon for a specific threat. Also, cost efficiency is vital for long-lasting defensive operations.

The Integrated Air and Missile Defence System (IAMDS) is complex and aims to fight against all air threats. This paragraph will focus on separate fighting methods against UAVs.

1.3.1. Drone-to-drone combat.

A new trend in antidot technology against drones is the development of drones capable of intercepting attacking drones and catching or disabling them by shooting nets at flying drones. Fully autonomous, radar-guided drone hunters can capture aircraft weighing up to 20 pounds (approximately 9 kilograms). It can also capture heavier aircraft, such as Iranian-built Shaheed 131 and 136 fixed-wing drones. (Sherman, 2023)

The good thing about the drone-to-drone method is that it does not involve bullets, missiles, or bombs. Collateral damage is reduced to the minimum. Specialised drones with the latest aerospace technology and the help of artificial intelligence can fire nets to target drones and jam their rotors. Eventually, drones will change their course and fall, or in the case of lighter target drones, they can be pulled back to the desired landing place.

Drone-to-drone combat could be cheaper in terms that drones would be cheaper than air defence missiles, and collateral damage could be smaller since the intercepting method would not use explosives. This method will require highly sophisticated radar systems capable of detecting and tracking drones. Due to the small radar cross-section, these radars will operate in a relatively small range of 10-15 km. Thus, this method will require good planning and employment in areas with high importance or the most dangerous enemy course of action places. The employment of this system could be improved by using passive sensors. To make this method effective, investment in research and development in self-learning artificial intelligence is still needed (Sherman, 2023).

1.3.2. Jamming systems

There are several methods to jam drone signals.

1.3.2.1. Global Positioning System GPS jammer.

GPS jammers are small devices that emit signals in frequency in the same way as GPS satellites. They interfere with the satellite signal, and the drone cannot determine its precise location and altitude. The result of this jamming can cause the operator to lose control over the drone, and it falls out of the sky (Cole, 2023). Advanced drones would turn to alternative guiding aids like visual aids supported by AI.

1.3.2.2. Frequency jammer.

A frequency jammer is a device that intentionally blocks or interferes with radio frequency transmissions. In some countries, it is not legal to use it since they could interfere with all devices using the same frequencies. However, for the drone, interference in its guiding frequency would mean that guiding signals are not received, the drone can lose its desired path, and the drone will require other aids to return home, or it can land or fall from the sky. If the frequency jammer is close enough to the drone

and jammers know the landing or order signals, then the drone can be diverted away from its initial trajectory or taken over and landed in the desired place (Cole, 2023).

1.3.3. Laser

Lasers can be used to blind the drone's optical sensors. In this case, if the drone is using a camera as one of its flying aids, it can lose its precision, recording malfunction or failure (Cole, 2023). Eventually, with the relatively cheap methods, the drones can be disturbed. Laser systems might require advanced radar and aiming aids.

Even though jammers could be considered one of the harmful methods of fighting drones, they have some disadvantages. Firstly, they might be illegal in most countries and require permission from the National Frequency Controlling Entity. Secondly, jammers could interfere with emergency responders and jam their communication systems. Thirdly, jamming the drone can cause jamming of other devices that are important for your own operations. Lastly, drones can fall out of the sky and cause damage to the civilian population (Cole, 2023).

1.3.4. Direct energy weapon

One of the latest developments in anti-drone technologies is the usage of direct-energy laser guns to destroy drones. As described above about lasers used for the destruction of optical devices on drones, this type of direct energy weapon uses the same method of detecting and tracking the drone but uses different wavelength laser beams to deliver high energy waves on an object to burn it. The system is effective, and tests showed the capability of intercepting small UAVs. However, the system is not automated yet, and it cannot determine UAVs from the birds. Also, direct energy weapons require a good source of energy to be able to output a 100 kW laser beam (Abrams, 2020).

1.4. What is Latvia doing in countering Unmanned Aerial Vehicles?

Latvia has prepared a comprehensive plan and has committed funds to procure systems providing defence capabilities against UAVs because of arising threats. However, air defence systems still need to be put in place (Media Relations Section, Latvian MOD, 2023). The Ministry of Defence of Latvia has included the defence of critical infrastructure as one of its top priorities in the States Defence Strategy (Latvian MoD, 2023).

One of the solutions which Latvia is acquiring from bilateral cooperation with the US is Northrop Grumman Corporation made Forward Area Air Defence Command and Control (FAAD C2) upgrade for existing Air defence equipment and addition with Counter- Unmanned Aerial System (C-UAS) capability (Northorp Grumman, 2021). The result of this bilateral cooperation will develop missing command and control mechanisms for the system to be connected to higher air defence echelons and provide the capability to positively control the unit. Positive control of the air defence unit is one of the prerequisites to conducting joint operations, getting support from allies in the same battlespace, and coordinating joint efforts. Through this bilateral program, Latvia integrates existing short-range air defence systems under FAAD C2. It will develop its capabilities to fight against threats towards small UAVs such as Shahed-136 to be capable of protecting critical infrastructure.

The sensors from all levels of air defence systems will contribute to common air picture production and improve common situation awareness in the air domain. Non-kinetic effectors such as signal jammers (FS-LIDS) will provide an effective alternative to engage UAVs.

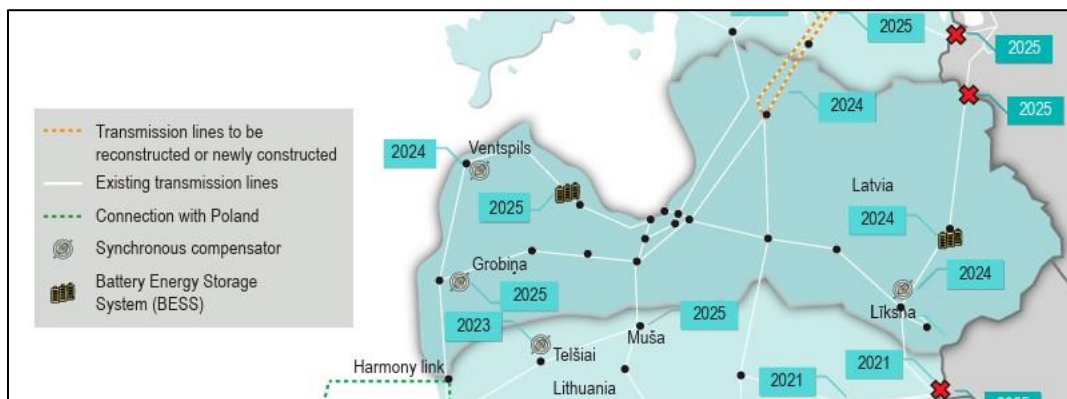
Procurement and implementation are just in the initial phase. Latvia plans to develop FS-LIDS capability combined with Very Short-Range Air Defence (VSHORAD) systems within every national Brigade-level unit as a Brigade-level asset. It will develop initial capability, from where Brigade level units could start to understand the application of systems and future need for development. In the implementation process, applying the system in the main effort of the Brigade's area of operations will be essential. This combination of non-kinetic and VHORAD systems will be a complementary layer to counter UAV threats.

1.5. Initial paragraph conclusion. Is it enough to survive future threats by Russia?

Latvia must possess a coherent Air and Missile Defence system (AMDS) to defend Critical Infrastructure. Some signs and projects mark the beginning of the development of such systems. Large numbers of objects and a lack of resources within the military will require military-civilian cooperation to put the responsibility to counter drones to

holders of critical infrastructure. The size of AMD units needed for Latvia can be planned based on the amount of electric CNI.

Latvia has a huge and advanced network of electricity lines and substations connecting them. There are 140 substations (including 330kV and 110kV) spread around the country (Board of the Public Utilities Commission, 2022). Most are around Riga, but others are spread in line to connect the power grid with Lithuania, Estonia, Sweden, and Belorussia.



Picture 1. Power grid network in Latvia (Board of the Public Utilities Commission, 2022)

An example of electric power grid object numbers shows that defence of them is challenging by military means alone. If every substation requires one AD battery as the lowest level of the tactical unit, then it will require at least 140 AD batteries (30 AD BNs would create 10 AD BDEs). Efforts to protect them should be combined with object holders, local law enforcement, and military unit capabilities. The number of AD units could be lowered by covering multiple objects under the coverage of one AD unit.

The National Armed Forces of Latvia must improve air defence capability rapidly. The air defence systems must be procured and developed, taking the lessons identified from the war in Ukraine. The numbers and size of air defence units must be revised. The defence of critical infrastructure against UAV attacks must be given as a task to brigade commanders as one of their objectives in the area of responsibility. Since such a capability will be available in Latvian armed forces, there is a question of whether that is enough and will the armed forces use it to protect critical infrastructure or if it will be a resource for force protection of troops. There should be a balanced approach,

and commanders having this resource should use their mastery of operational art and find the best suitable use of the system.

2. Countering long-range threats

2.1. Actuality of threat

Long-range missile threat is one of the most dangerous threats towards critical infrastructure. For a small state like Latvia, it is problematic that there is no depth in defence. Russian missiles can reach any place in Latvia's territory. The lethality of this threat is that it is hard to detect launch and even harder to counter ballistic missiles without a specific air defence system. Ballistic missiles are very precise and can carry a heavy warhead that causes massive damage towards infrastructure. Even though ballistic missiles are expensive to produce, the effect gained by destroying critical infrastructure objects can be strategic and change the course of battle.

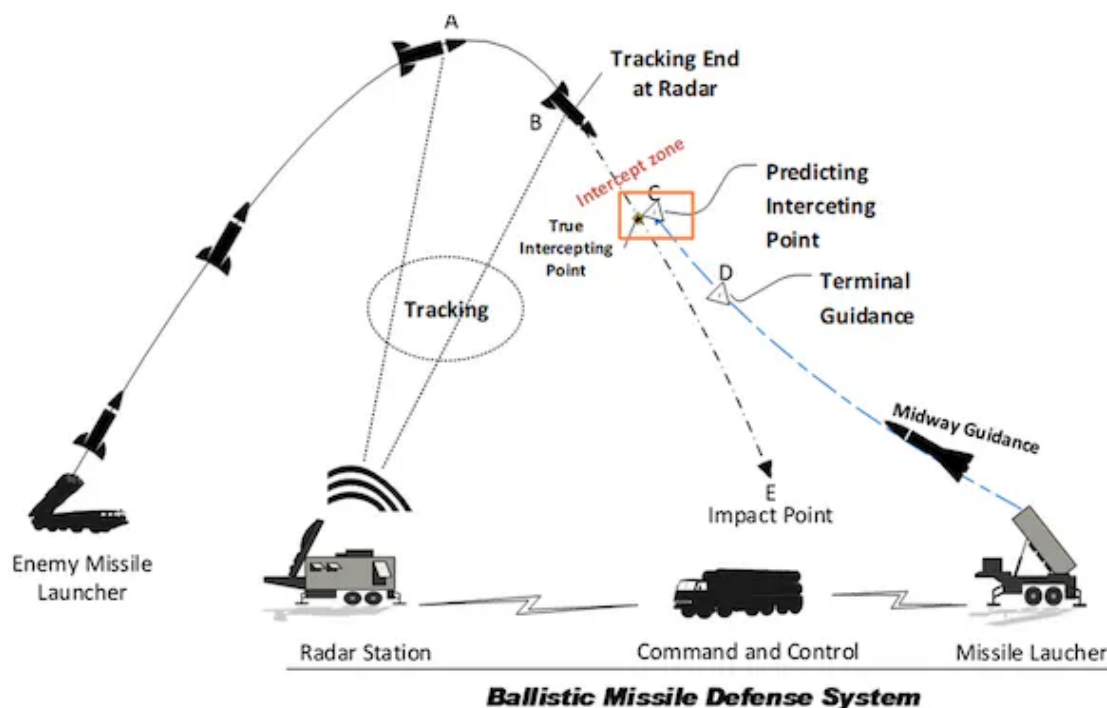
2.2. Description of the threat

Russia possesses a variety of long-range missile systems, including intercontinental ballistic missiles (ICBMs) and cruise missiles. They were massively used against Ukraine in the initial attack and, at certain times, in waves used for destroying military targets and mostly Critical National Infrastructure. Since the beginning of the war in Ukraine, Russia has launched over 1524 cruise missiles (Umerovs, 2023). Over the time of war in Ukraine, Russia ran out of stocks and decreased its use of long-range missile systems. However, Russia managed to produce missiles despite sanctions on the delivery chain of important components of missiles.

The main strategy of using missiles by Russia is to target infrastructure and objects which are of strategic importance of Ukraine. As reports show, the main destruction is caused on factories, critical energy infrastructure, and civilian living area (Harmash, Balmforth, 2023). Missiles often are fired in well-coordinated massive attack waves, 10 to 50 missiles at a time, after the Shaheed drone wave that has exhausted or overwhelmed the Ukrainian air defence system. After breaching the air defence bubble, missiles are launched to hit targets of high importance and with such great devastation that restoration of destroyed critical infrastructure is taking far greater time than after the attack of a Shaheed drone.

Initially, the pattern of Russia using missiles showed that they were targeted at strategic targets which directly or indirectly supported Ukraine's military activity. Now, after Russia failed to reach significant military goals, its strategy of using Tactical Ballistic Missiles (TBMs) and Cruise missiles has changed to a "burn the land" strategy, where Russia is targeting everything. Starting from military targets and factories that produce material for the army, including food and civilian urban areas and apartment buildings, to demotivate support for the population.

To understand the threat from ICBMs, it is crucial to know how they are employed and the differences in countering them. Firstly, ICBMs are launched far behind the radar coverage of Ukraine or allied radars, and it is tough to detect the launching stage of the missiles. Secondly, they fly at high trajectory and great speed. Due to this difference in the launch and flying trajectory from cruise missiles, there is a need for specialised additional or specially allocated units to perform counter-ballistic missile operations,



Picture 2. Fundamental elements of missile defence (Boyd, 2022).

Most radars are tuned for detecting aircraft, and automatic detection and tracking systems are set to these conditions for speed and altitude. It leads to the last point that Ukraine must use a specially assigned air defence system which focuses on finding and tracking the re-entry phase of the ICBM launch sequence and, in a matter of seconds, must counterfire to destroy the ICBM successfully.

It takes a massive effort to defend vast areas of Ukraine and counter tactical ballistic missiles. Due to the remarkable speed of ballistic missiles and high-altitude trajectory, most air defence systems capable of countering ballistic missiles can defend relatively small areas. This means that counter-ballistic missile (C-BM) systems should be deployed for objects or places that are highly valuable.

Other long-range threats, like cruise missiles, can be countered with conventional Surface Based Air Defence (SBAD) Medium Range Air Defence (MRAD) systems provided by the US and Germany. Ukraine has deployed significant layered air defence, consisting of Short-Range Air Defence (SHORAD), MRAD and C-BM defence systems within crucial areas and over most dangerous avenues of approach.

2.3. What is the other world doing? New systems, current approaches, new ideas/tendencies.

Great Power military is spending its defence budget and investing its resources in research and developing new methods and systems for air defence systems against long-range missile threats to protect its own CNI.

2.3.1. Multi Domain Air Defence

The US has a good example of the development of Multi Domain Air Defence. They spend huge resources on research and development and are ready to share technology with their allies, who are prepared to cooperate and invest.

“The Integrated Air and Missile Battle Command System (IBCS), developed by Northrop Grumman under a contract from the U.S. Defense Department, is also essential for the Polish Armed Forces. It has been acquired in the first phase of the Wisła air defense program, along with Patriot Air Defense systems. IBCS is based on the principle „any sensor, best effector” and can combine various components of the air defense system to include medium and short-range systems. That is why its application can be extended.”(Palowski, 2021)

2.3.2. Advanced Sensor Technologies

As disclosed in the article, the focus is on multi-domain integration. All radars from Land Component, Coastal defence systems and NAVY AEGIS ships contribute to air picture generation (Palowski, 2021). Since the systems have become digitalised, they have become better integrated into *The Integrated Air and Missile Battle Command System* IBCS. Effectors from ships and Patriot systems from the ground have been tested against targets together with new F-35 aircraft, and they proved effective against long-range missile threats.

Poland has joined this cooperation and is developing Multi Domain Operation IBCS. Advancements in sensor technologies and the digitalisation of systems have made it possible to integrate SHORAD systems into IBCS as well. That offers additional options to decision makers to use a proportional air defence system against smaller targets if necessary.

2.3.3. Capability of military industry

The rising threat situation asks countries to create new air defence units. The military industry is asked to develop and build new systems. Since this capability is in high demand and production capability is low, it increases the price of air defence systems. That consequently puts countries' budgets under stress. To compensate, countries are developing local military industries and focusing on producing military goods to ensure delivery security and keep part of the invested money inside the country.

2.4. What is LVA doing? LVA approach, ideas (projects).

With the increasing threat from Russia, including long-range missile threats, the Latvian government has allocated funds to procure IRIS-T medium-range air defence system (MRAD) capable of intercepting the ballistic missiles (Media Relations Section, Latvian MOD, 2023).

So far, Latvia has no AD resources capable of intercepting long-range threats. This capability gap is mitigated by Baltic Air Policing (BAP) and MRAD units deployed to Latvia after the government requested NATO to support the Eastern flank of NATO. Since a small country like Latvia cannot counter long-range missile threats, the Latvian approach to solving this will mainly rely on support from NATO nations willing to contribute to developing Latvian capabilities. In this approach, Latvia has requested

MRAD units to deploy in Latvia, and Spain has sent one MRAD (NASAMS) unit to defend Lielvarde AFB, which is part of NATO Integrated Air and Missile Defence System (NATINAMDS) (Allied Air Command Public Affairs Office, 2023). Spanish units provide MRAD capability, share their experience, and help LVA Air Force initiate and develop their own MRAD capability. Bilateral cooperation in this area is expected to last until Latvia acquires their own MRAD capability. The deployment time of the Spanish MRAD unit is prolonged by the Spanish government periodically and based on threats. The Spanish MRAD unit might stay in Latvia even after Latvia has developed its own MRAD capability to transfer knowledge and experience of the application of the MRAD system.

2.5. Initial paragraph conclusion. Is it enough to survive future missile threats by Russia?

As a small state, Latvia will face difficulties in countering Russian long-range attack threats without support from NATO. Latvian air defence capabilities are underdeveloped and will need assistance from nations with this capability. Latvia must proceed with its plan to procure and make an operational medium-range air defence system as part of the NATO integrated air defence system.

To reach significant air defence capability, Latvia must cooperate with nations with advanced AD capabilities, such as the US and Spain. Cooperation with more advanced countries with decent air defence systems employed and used in practice should provide knowledge and best practices on making the air defence system effective against long-range threats.

Military mission planning must involve coordination with local or national-level owners of critical infrastructure to understand better the possible influence of losing or damaging critical infrastructure on the battle space environment. Destruction of critical infrastructure can influence a nation on a strategic level. That is a reason why the protection and resilience of critical infrastructure should be done with a comprehensive approach. Military and civilian entities together.

Passive methods, like dispersal and hardening, must be applied to protect CI from long-range missile threats. Dispersal is a common method applied in the military to

separate dangerous or vital assets in a distance that could not damage more than one unit with one shell. Hardening is a method used to cover and conceal high-value material with ground or concrete material to lower damage caused by explosives or shrapnel. In the case of energy infrastructure, both passive methods could be combined to lower the risks of damaging multiple vital elements in the system. Already built objects can be fortified by blast walls in the form of concrete T-walls. New energy infrastructure must include passive protection measures in the planning and designing process.

Lastly, the Latvian army can develop a good backbone of a pre-deployed C2 system that is interoperable with partner systems and can be utilised in future. Existing stationary and mobile radar systems can be connected to the C2 system and contribute to recognised air picture (RAP). At the same time, the Air Force can develop and practice system connectivity and interoperability procedures. This way of interoperable network development could prepare NATINAMDS elements to be delivered and reach full operational capability faster.

Conclusion and Recommendations

Latvia has a significant number of CNI objects. Detailed information is sensitive. However, official plans for the development of the energy sector show that there are at least 140 high-voltage substations dispersed across Latvia and connecting Baltic states in one network. Considering a number of other CNI objects, it is a joint effort of the military and other governmental agencies to plan the protection and security of objects.

There should be a balance between operational and capability-based planning methods for force planning and the spread of the units in Latvian territory. AD units must be developed with high priority, and the structure of unit dispersal should be revised constantly to find the most effective ways of employing the AD system.

Additionally, to develop classical AD units, Latvia must invest and cooperate with partners (for example, The US) to develop anti-dot against drones. Latvia should develop a counter-UAV system that can counter UAVs precisely without depleting Air defence resources designed against bigger targets. The complementation of electronic means to kinetic countermeasures against drones is vital to save missile resources

and lower collateral damage. Since there is no universal system against UAVs, Latvia should continue to develop plans and procure various weapons like smart munition guns, small missiles and electronic warfare systems that could effectively counter UAVs.

Latvia must proceed with its plan to procure and make an operational medium-range air defence system as part of its integrated air defence system. By implementing a medium-range air defence system, Latvia must cooperate with Spain, which has deployed medium-range units in Latvia Lielvarde Air Force Base, to gain knowledge and learn best practices for using the system and making it effective against long-range threats.

Latvia must create UAV units capable of performing defensive and offensive capabilities. The creation of a UAV unit will help to develop an understanding of UAV's capabilities and will boost research and development in this area.

In parallel with the procurement and development of a physical air defence system, the Latvian Air Force can develop a conceptual framework of the system, which is Air defence doctrine for the operational level and use of MRAD. This development of the conceptual part of the AD system will broaden the understanding of AD within the armed forces. AD units from Spain, Italy and the US deployed in Latvia as part of eFP can contribute to the development of a conceptual framework and understanding of the application of AD at most. Since eFP units have deployed to Latvia on a rotation basis, it could be a beneficial training opportunity.

Cooperation with Spanish MRAD units within exercises can broaden the understanding of the application of air defence in the Latvian army. At the same time, air defence Command and Control (C2) integration can be employed. The backbone of C2 networks is important in air defence integration to NATINAMDS. The air defence unit deployment to Latvia and connectivity to the Combined Air Operation Centre (CAOC) is a good signal for the future development of the Latvian MRAD system. Contribution to NATINAMDS is important for future air defence unit deployments to Latvia in case of crisis.

Additionally, to military development efforts a comprehensive whole government approach, Latvian CNI holders should use the advice of the military and add passive AD methods to existing CNI. Also, passive AD methods like dispersal and hardening should be applied during the planning and construction of new CNI. Both methods could be applied separately; however, when there is limited space for dispersal, it can be compensated with underground locations of CNI objects or blast wall separation.

For the CNI objects like electric wind farms, compensatory elements for air surveillance coverage should be included in the project planning phase. Even though it is increasing the costs of the project, compensatory elements should be financed by the project developer as their responsibility to protect the infrastructure piece in case of possible armed conflict. This concept is vital to compensate for the possible infiltration of enemy aircraft under the cover of windmills.

Bibliography

ABRAMS, Michael. 2020. Laser Weapon to Shoot Down Drones - ASME. [Online]. 1 October 2020. [Accessed 11 February 2024]. Retrieved from: <https://www.asme.org/topics-resources/content/laser-weapon-to-shoot-down-drones>

ALLIED AIR COMMAND PUBLIC AFFAIRS OFFICE. 2023. Air defence: Spanish NASAMS system comes online in Latvia. [Online]. 18 April 2023. [Accessed 22 February 2024]. Retrieved from: <https://defence-industry.eu/air-defence-spanish-nasams-system-comes-online-in-latvia/>

BBC NEWS. 2023. How are “kamikaze” drones being used by Russia and Ukraine? *BBC News*. [Online]. 29 October 2023. [Accessed 4 October 2023]. Retrieved from: <https://www.bbc.com/news/world-62225830>

BOARD OF THE PUBLIC UTILITIES COMMISSION. 2022. *Electric Transmission Development plan. 2023-2032*. [Online]. 25 May 2022. [Accessed 12 February 2024]. Retrieved from: https://www.ast.lv/sites/default/files/editor/AST_10GAP_2023_2032_ENv6.pdf

BOYD, Iain. 2022. A game of numbers: How air defense systems work and why Ukraine is eager for more protection. *The Conversation*. [Online]. 18 October 2022. [Accessed 10 October 2023]. Retrieved from: <http://theconversation.com/a-game-of-numbers-how-air-defense-systems-work-and-why-ukraine-is-eager-for-more-protection-192487>

COHEN, Raphael S., CHANDLER, Nathan, EFRON, Shira, FREDERICK, Bryan, HAN, Eugeniu, et al. 2020. *The future of warfare in 2030: project overview and conclusions*. Santa Monica, Calif.: RAND. ISBN 978-1-977402-95-0.

COLE, Jamie. 2023. How To Jam Drone Signals (4 Effective Methods). [Online]. 25 August 2023. [Accessed 11 February 2024]. Retrieved from: <https://discoveryoftech.com/how-to-jam-drone-signals/>

FRIDBERTSSON, Njall Trausti. 2022. *TECHNOLOGICAL INNOVATION FOR FUTURE WARFARE*. . 20 November 2022.

HAGEN, Isobel van. 2023. Russia is using a new delivery of Iran's Shahed drones to strike Ukraine to make up for a lack of precision munitions, reports say. *Business Insider*. [Online]. 23 April 2023. [Accessed 10 February 2024]. Retrieved from: <https://www.businessinsider.com/russian-troops-shahed-kamikaze-drones-latest-ukraine-attack-2023-4>

HARMASH, Olena and BALMFORTH, Tom. 2023. Russia hits Ukrainian energy facilities in biggest attack in weeks, Kyiv says. *Reuters*. [Online]. 21 September 2023. [Accessed 23 September 2023]. Retrieved from: <https://www.reuters.com/world/europe/blasts-heard-kyiv-other-parts-ukraine-2023-09-21/>

HAYNES, Deborah. 2024. "Explosive" new attack drone developed by Iran for Russia's war in Ukraine. *Sky News*. [Online]. 1 October 2024. [Accessed 10 February 2024]. Retrieved from: <https://news.sky.com/story/explosive-new-attack-drone-developed-by-iran-for-russias-war-in-ukraine-13045093>

LATVIAN MOD. 2023. *States defence concept*. [Online]. 2023. Retrieved from: https://www.mod.gov.lv/sites/mod/files/document/AM_VAK-2023.pdf

MEDIA RELATIONS SECTION, LATVIAN MOD. 2023. Latvia and German company "Diehl Defence" sign purchase order on procurement of the IRIS-T medium-range air defence system | Aizsardzības ministrija. [Online]. 30 November 2023. [Accessed 10 February 2024]. Retrieved from: <https://www.mod.gov.lv/en/news/latvia-and-german-company-diehl-defence-sign-purchase-order-procurement-iris-t-medium-range>

NORTHROP GRUMMAN. 2021. Northrop Grumman FAAD C2 to Provide the Baltics Full Interoperability with NATO Air Defense Architecture. *Northrop Grumman Newsroom*. [Online]. 14 December 2021. [Accessed 2 October 2023]. Retrieved from: <https://news.northropgrumman.com/news/releases/northrop-grumman-faad-c2-to-provide-the-baltics-full-interoperability-with-nato-air-defense-architecture>

PALOWSKI, Jakub. 2021. IBCS as the Foundation for Multi-Domain Air Defense. [Online]. 24 September 2021. [Accessed 22 February 2024]. Retrieved from: <https://defence24.com/armed-forces/bcs-as-the-foundation-for-multi-domain-air-defense>

SAEIMA OF LATVIA. 2023. *Nacionālās drošības likums*. [Law of national security] [Online]. 1 January 2023. Saeima. [Accessed 30 January 2024]. Retrieved from: <https://likumi.lv/doc.php?id=14011>

SHERMAN, Jason. 2023. Drone-on-Drone Combat in Ukraine Marks a New Era of Aerial Warfare. *Scientific American*. [Online]. 4 March 2023. [Accessed 11 February 2024]. Retrieved from: <https://www.scientificamerican.com/article/drone-on-drone-combat-in-ukraine-marks-a-new-era-of-aerial-warfare/>

UMEROVS, Rustems. 2023. Umerovs: Ukraina atbildēs uz Krievijas uzbrukumiem enerģētikas infrastruktūrai. [Ukraine will respond to Russian attacks on energy critical infrastructure] *Delfi LV*. [Online]. 27 September 2023. [Accessed 27 September 2023]. Retrieved from: <https://www.delfi.lv/46713439/arzemes/55977316/umerovs-ukraina-atbildes-uz-krievijas-uzbrukumiem-energetikas-infrastrukturai>

ZOIA KURTANIDZE. Can the Feminization of Leadership Improve National Security?

Introduction

International peace and security face a broad spectrum of challenges in an era of rapid technological development and shifting geopolitical landscapes. While international armed conflicts and terrorism persist, hybrid challenges, such as cyber-attacks, weaponised migration or energy security threats, intensify the complexity of the security environment. Beyond traditional defence methods, various security threats require diverse, collaborative, holistic approaches to respond resolutely. Due to current threats, the traditional conception of security, once predominantly associated with military might, has evolved to encompass more factors related to humans (Arostegui, 2015 p. 15).

In 2000, the United Nations Security Council adopted Resolution (UNSCR) 1325, 'Women Peace and Security'. This resolution recognises the disproportional impact of armed conflict on women, including conflict-related sexual and gender-based violence (CRSGBV). UNSCR 1325 advocates for higher representation of women in decision-making, especially in male-dominated security domains. UNSCR 1325 is a policy directive which ensures that women leaders enrich perspectives and solutions through diverse backgrounds and perspectives (United Nations Security Council (UNSC), 2000). Five years later, the United Nations General Assembly (UNGA) adopted a resolution 60/1 '2005 World Summit Outcome' on development, security, and human rights and initiate the definition of human security (United Nations General Assembly (UNGA), 2005). In 2012, the UNGA adopted a follow-up resolution on human security, recognising its tight linkage to peace and human rights. Resolution defines human security as 'addressing widespread and cross-cutting challenges to the survival, livelihood and dignity of their people' (United Nations General Assembly (UNGA), 2012). After a decade, in 2022, the North Atlantic Council (NAC) established 'The Human Security Approach and Guiding Principles' at the Madrid Summit. These principles reflect the North Atlantic Treaty Organization's (NATO) core values of 'individual liberty, human rights, democracy, and the rule of law' (North Atlantic Treaty Organization (NATO), 2022).

In the context of EU and NATO human security resolutions, along with current and future possible threats, an intriguing perspective becomes apparent: the potential for the feminization of leadership to redefine the traditional leadership approach.

The feminization of leadership is an initiative to shift leadership approaches and methodologies from traditionally masculine-dominated to inclusive and all-encompassing. It emphasises the broader employment of human-centric methods in leadership, such as empathy, collaboration and emotional intelligence. The feminization of leadership mainly means utilising traditionally feminine traits in leadership tactics (Fondas, 1997 p. 260). The trend includes transformation in leadership approach and the rising number of women leaders, especially in male-dominated areas. In addition, the feminization of leadership does not exclude men from leadership, as these traits are not exclusively feminine. However, it refers to more cultural and social change based on customers' and workforce needs and requirements.

This research paper aims to demonstrate that the feminization of leadership, through its human-centric approach, significantly enhances national security, making it more peaceful, safe and resilient to contemporary and future threats.

Although there is extensive research on women leaders in organisations globally, the empirical research gap in security exists due to the lack of female leaders in the military sector. Due to the significant similarity between the feminization of leadership and transformational leadership, I will use the latter as a foundational framework to enrich analysis and discussion.

Initially, I will briefly review the development of leadership theory to create a foundation to examine the feminization of leadership. Next, by analysing gender dynamics, I will illustrate how cultural norms affect women, especially in male-dominated areas, to pursue a career in leadership. Finally, I will conclude the discussion with the feminization of leadership outcomes in security, supported by persuasive evidence and meta-analysis reviews.

Brief Overview of The Leadership Theories

Over time, theorists and scholars shaped and developed the concept of leadership from the perspectives of each era. Despite the constant development, the definition of leadership remains elusive. As Ralph Stogdill remarked, 'There are almost as many definitions of leadership as there are persons who have attempted to define the concept' (Stogdill, 1974 p. 259).

From ancient leadership theories to modern ones, leadership fundamentally revolves around the individual's ability to influence followers. Across diverse leadership theories, influence consistently appears as a core element of leadership to guide the followers toward success. However, according to Gary Yukl, influence extends beyond the ability to affect actions and emphasises the ethical dimensions to influence followers (Yukl, 2006 pp. 4-5).

Leadership theorists focus on characteristics and how leaders can effectively influence their followers. The debates begin with the ancient philosophers who noted the traits of influential rulers. For instance, in his concept of 'philosopher-king', Plato highlights qualities such as wisdom, knowledge, and virtue and advocates ruling beyond personal interests and the material realm. However, this approach to influencing followers was criticised for its idealistic approach, ignoring human nature and inclusive leadership (Zannat, et al., 2020 pp. 42-43). Centuries later, Thomas Carlyle shifted his focus towards innate qualities in 'The Great Man Theory'. He suggested that leaders are gifts from heaven, born with inherent charisma, heroic courage, and 'light, which lightens the dark', enabling them to shape the world (Carlyle, 1906 p. 2). It is essential to acknowledge that Carlyle's 'The Great Man Theory' is a gender-biased approach, which excludes women from leadership and reinforces gender stereotypes. Continuing Carlyle's approach to the inherent traits of leaders, Trait theory, with multiple authors, suggests that traits, such as visual characteristics and intelligence, are inherent and based on heredity. This explains why leaders are distinguished from non-leaders, enabling them to influence followers. However, trait theory also suggests that some traits can be learned and experienced. In contrast, in the late 20th century, Contingency (Situational) Leadership theory asserts that a leader's effectiveness depends on the ability to adapt. According to this theory, there is no universal approach, as situation, team, quality, and other variables are different. An effective leader is determined by whether the leader's flexibility and agility fit the context. Another theory, known as Behavioural Leadership Theory, focuses on the ability of leaders to adopt relation

methods based on followers. Behavioural leaders influence effectively by prioritising people and relations (Khan, et al., 2016).

The 20th century was a sociology-striving era. Despite becoming sociology as an autonomous discipline in the 19th century, sociologists actively started scientifically exploring societies, societal groups and organisations in the next century. The sociological framework became an analysis tool to widely understand diverse processes and human-related aspects (Calhoun, et al., 2007 pp. 13-14). On the other hand, psychology, as a distinct scientific discipline, extensively examines individual behaviours and cognitive processes, especially from the 20th century. The focus included underpinning emotional mechanisms as a tool which affects one's and others' hearts and minds and shapes human behaviour (Passer, et al., 2007 pp. 338-339).

Both sociology and psychology frameworks enriched the analysis of leadership theory to understand the dynamics of organisations and individuals. Notably, the role of emotional intelligence in psychology reshaped existing leadership theories and emerged new ones grounded on emotional intelligence. As a result, mid- and late-20th-century leadership theories encompass broader ethical, emotional, and social aspects critical to successful leadership. The current focus is on followers and how to develop and motivate enthusiastic employees to ensure organisational success. This approach underpins the importance of social and emotional aspects, which are one of the core bases of effective leadership, one way or another (Yukl, 2006 pp. 152-153). The approach that heavily integrates social and emotional aspects is known as transformational leadership. First established by James Burns in 1978 and developed by Bernard Bass, transformational leadership leads the company with an inspiring force which stimulates followers to 'achieve extraordinary outcomes' (Bernard M Bass, 2006 p. 3). Researchers find that emotional intelligence, such as empathy and social responsibility, have a high role in the success of companies, as leaders present trust and commitment beyond their immediate self-interest, driving advanced performance for the greater good (Sayeed, et al., 2009 pp. 594-595).

Transformational leadership has remarkable effectiveness in creating a positive work environment. When leaders present a transformational approach, followers experience enhanced inspiration, motivation, satisfaction and performance, demonstrating a notable alignment with improved outcomes (Bernard M Bass, 2006

pp. 4-5). Leaders transcend their interests and champion the team's and organisation's shared goals, activating their higher-order needs. In responding, followers demonstrate trust, respect and solid loyalty to their leaders (Yukl, 2006 p. 321). This fosters an environment that promotes creativity and resolves challenges.

Although the feminization of leadership incorporates elements of various modern leadership theories, such as motivational, servant or charismatic leadership theory, it is mainly best aligned with transformational leadership, which is more than a theoretical examination; transformational leadership is a practical approach to evolving leadership models to be more inclusive and effective.

The correlation between the feminization of leadership as a process and transformational leadership as an approach - promises to redefine traditional notions of influence and authority. This marks a significant shift towards more holistic and inclusive leadership practices that benefit organisations and pave the way for a more balanced and dynamic approach.

The Concept of the Feminization of Leadership

Demographic, economic, and competitive changes in today's workplace impose new, non-traditional leadership behaviour, which implies breaking the boundaries of the traditional framework. Modern leaders are encouraged to share responsibility, help others, and develop networks to succeed. Although authors in the scientific literature avoid calling this leadership style feminine, it inadvertently emphasises culturally feminine qualities (Fondas, 1997 pp. 257-258).

Generally, feminization means that 'something or someone that was not previously feminine has become feminine' (Imhoff, 2016 p. 126). In terms of leadership, it suggests a shift from traditional leadership approaches, which often prioritise hierarchy, assertiveness and competition, to ones that exercise team-oriented methods. Besides empathy and active communication, the human-centric approach includes building team cohesion, fostering follower's motivation, and mentoring-based development. Similarly to transformational leadership, the feminization of leadership utilises emotional intelligence, understanding its crucial role in leading organisations in complex, rapidly changing situations (Fondas, 1997 p. 260).

People traditionally associate qualities such as active communication, collaboration, empathy, fostering motivation, and mentoring-based development with women (Suciu, et al., 2023). This is why the exhibition of feminine characteristics in leadership approaches is mentioned as the Feminization of leadership.

Another explanation of the feminization of leadership refers to the rising presence of women leaders in spaces dominated by men, either for the first time or with a rising number. This egalitarian process sometimes has a negative connotation. Some sources describe this process as the 'absence of men', noting that the increased number of female leaders proportionally decreases the number of male leaders (Imhoff, 2016 p. 128). Men are traditionally seen as leaders in societies with deeply ingrained stereotypes and perspectives. Cultural change is a gradual process and poses challenges for women to aspire to as leaders. However, this is an inevitable and essential process to respond to human rights and gender equality, considering that women comprise half the global population.

The concept of feminization leadership is still evolving and has not been defined or widely accepted in the academic environment. The feminization of leadership and transformational leadership emerged around the same period in the 20th century (Fondas, 1997 p. 258). However, despite the enormous similarities in leadership approach, methods and characteristics, the feminization of leadership has not gained popularity due to cultural norms and social implications. In addition, related to cultural norms, Billing and Alvesson noted that some leadership traits, such as prioritisation of feelings, creativity, encouragement of others and sharing power, come from the early childhood of women, as they are taught to care for others while men are taught to fend for themselves (Billing, et al., 2000 p. 148). It suggests that cultural norms may lead to women being more transformational leaders than men.

Scholars on Women's Transformational Leadership

Based on Bass and Riggio's meta-analysis, women exhibit attributes commonly linked to transformational leadership as they demonstrate high levels of empathy, the ability to motivate followers and foster intellectual development (Bernard M Bass, 2006 p. 112). This observation aligns with other scholars and researchers who similarly

recognised women's transformational leadership traits and methods. Diane Chandler notes that women leaders create collaborative environments with diverse perspectives to maximise the contribution and capabilities of all members and organisations (Chandler, 2011 p. 7). Eagly and Carli note that women exhibit advantages due to their supportive and considerable behaviours. However, social norms and gender expectations, especially in male-dominated organisations, do not benefit them to become leaders (Alice H. Eagly, 2003 p. 825).

Based on Dr. Alice Eagly's research, Anna Gorska suggests that women leaders are more transformational than their male counterparts. Women leaders focus more on participative and democratic ways of leadership, focusing on communication, cooperation, and affiliation than men, meaning they are more collective-centric (Gorska, 2016 p. 138).

Women exhibit more transformational leadership mainly because of their massive sense of emotional intelligence. This trait is critical in transformational leadership, which is divided into four key pillars known as 'I' factors: Idealized influence (II), inspirational motivation (IM), intellectual stimulation (IS), and individualised consideration (IC). Based on studies conducted in 1986-1992 in different countries and companies, Bass suggests that female leaders attain higher scores in all four pillars of transformational leadership than their male counterparts (Bernard M Bass, 2006 p. 117). Similarly, Eagly, Van Engen and Johannesen-Schmidt proved that women are most likely to be transformational leaders among the different types of leadership. They scored higher in all components of transformational leadership than their male colleagues. The finding is based on a comprehensive meta-analysis conducted in 2003, where 45 studies were examined (Bernard M Bass, 2006 p. 120)

By applying these pillars, leaders can create an organisational climate that enables followers to feel motivated and find themselves valuable contributors to the team. Under the first pillar, idealised influence, leaders prioritise followers' needs over their own. They become examples of courage and dedication, making them role models for their followers. Second, inspirational motivation is another dimension where leaders challenge and inspire followers. They project a meaningful and compelling future vision and encourage the team to work enthusiastically to achieve the goals. Third, intellectual stimulation fosters followers' creativity and innovation. Followers' critical

thinking and problem-solving approach generate ideas which benefit organisations with a competitive advantage and increased efficiency. The fourth pillar, individualised consideration, showcases leaders' high level of empathy and support. Through mentoring and coaching, leaders individually attend to followers' needs. This approach promotes a bolstered degree of career development (Stepanek, et al., 2022 pp. 1-2).

By demonstrating 'I' factors, women leaders enhance teamwork and authentic communication as prerequisites for success. In addition, they promote cooperation and conflict-free relations between employees. Women often communicate their expectations, demonstrating trust towards followers and allowing them the freedom to achieve their goals. This approach consists of core elements of mission command. Mission command is a military approach to leading forces in operations that suggests centralised planning and decentralised execution. Under the mission command approach, subordinates are encouraged to take the initiative and exercise freedom of action within defined constraints (NATO Standardization Office, 2022 p. 42).

In conclusion, women leaders excel in transformational leadership, which is lauded for manifesting a human-centric approach. Various sectors, including security, favour transformational leadership due to its human-centric approach; however, trust in women leaders is still low. In other words, while there is a high demand for feminine qualities in leadership, female leaders' acceptance remains reluctant. Gender and cultural norms are crucial in shaping attitudes toward leadership roles and acceptance.

Gender and leadership

Theorising leadership is not gender-neutral; gender and leadership are closely interrelated concepts. Usually, the former determines the latter. Traditional gender roles in society determine the behaviour. Gender, as social and cultural differences between males and females, affects people thinking about themselves or others. Gender affects every aspect of an individual's life, including leadership representation and acceptance.

Gender conceptualises attributes, behaviours, and roles, mainly for men and women, and societal norms, beliefs, and values influence these. The gendered division between men and women is described into two main concepts: 'masculinity' and

'femininity'. Those two are related to female and male bodies and are often seen as mutually exclusive. These categories are defined by culture, tradition, and social construct, not by biological necessity. They are created from a dynamic, interconnected cognitive, emotional, and social complex (Billing, et al., 2000).

Based on traditional gender roles, leadership has been chiefly spinning around men and masculinity, especially in the security sector. According to this, male roles have been typically recognised as more congruent with leadership roles than females (Brenner, et al., 1989). Contextual and other factors primarily influence perceptions of leaders, and leaders' actual behaviour is often a pure reflection of their beliefs based on gender. Understanding society's fundamental convictions is essential to understanding how context interacts with these beliefs.

Gender also affects language. For instance, 'think manager, think male' or 'think manager, think masculine' encapsulates broadly observed stereotypical attitudes toward leadership (Van Engen, 2001 p. 22).

A typical description of masculine leadership emphasises objective, action-oriented, analytical, linear, rational and materialistic characteristics. Leadership principles include assertiveness, autonomy, control and competition, which are culturally coded as masculine (Billing, et al., 2000). Similarly, Shane's study examined that society's expectations of leadership qualities confirm that they are primarily associated with masculine characteristics (Brenner, et al., 1989).

At the beginning of the 20th century, masculinity and femininity were conceptualised as two opposite ends of leadership. Based on Van Engen, in 1936, Termand and Miles's work, feminine and masculine traits are explained by antonyms. Rationality, insensitivity and coldness are stereotypically associated with males, while irrationality, sensitivity and warmth characterise females. Such differences and the labelling of male or female leadership created barriers for women in leadership roles. They kept women in socially constructed roles as housewives or at lower-income jobs (Van Engen, 2001 pp. 22-23).

Women often face prejudices and biases that undermine their competence. The persistence of this discrepancy may be ascribed to long-standing societal prejudices

regarding the capabilities of women, particularly in traditionally male-dominated domains like national security. In such an environment, obstacles become especially conspicuous for women, given that males generally occupy more influential positions. This bias significantly influences women's advancement (Alice H. Eagly, 2003 p. 818).

Gender affects not only women's development but also assessment. Evaluations of women's leadership capabilities are often subject to bias, especially in male-dominated environments. Even when women's performance is objectively equivalent to or surpasses their male counterparts, they often receive lower assessment or negative feedback. According to a meta-analysis by Eagly, Makhijani, and Klonsky, male evaluators tend to attribute lower ratings to female leaders than male leaders of equivalent standing. In contrast, female evaluators do not exhibit this gender bias. The discrepancy mentioned above highlights the impact of gender bias on leadership evaluations and the subsequent repercussions for the progression of women, especially in national security-related fields (Alice H. Eagly, 1992 pp. 819-820). Similarly, Bernard Bass notes that perceptions and biases affect the assessment of leaders. It advantages men leaders and disadvantages women leaders. In 1985, 12 men and 12 women leaders from Fortune 500 firm participated in training workshop on transformational leadership. They were described by 3-5 subordinates following the Multifactor Leadership Questionnaire (MLQ). Leaders' gender, age or any information about their identification was not provided. Despite the expectation of research participants that at least 2, in not all 4, would be men, it turned out that all four leaders were women, who had the highest score of charisma; they were 'top-rated leaders by a sizable margin' (Bernard M Bass, 2006 p. 115). According to the preliminary assumption of the participants in this study, if subordinates knew whose profile they were evaluating, it would change the overall assessment and picture.

Preference for men in leadership roles, stereotypically associated with masculinity, does not favour women leaders. They face barriers to attaining such positions, yet they significantly contribute to national security. In this point of view, femininity is insufficient for leadership, as it does not fit into the traditional masculine framework. This may be considered one of the main reasons for the low popularity of the feminization of leadership. However, gender-constructed social processes are complex, multifaceted and heterogeneous, as femininity or masculinity is not static; it varies over time

according to class, race, occupation, organisation, age, and individual circumstances (Billing, et al., 2000 p. 146).

Despite its long history of masculine traits in leadership, the demand for significant transformation has evolved. Due to the widespread popularity of the human-centric approach, which spans sectors such as business, education, healthcare, and security, the feminine element is becoming appreciated in the leadership approach.

The Feminization of Leadership, Women and Security

The actuality of examining the feminization of leadership in security derives from adopting the human security approaches in NATO and the EU. The 21st century, marked by its diverse challenges, signifies a transforming era due to adopting human security resolutions. UNSCR 1325 champions women's participation, women leaders and inclusivity in peace and security. UNGA resolution 60/1 (2005) and follow-up resolution 66/290 (2013) emphasise the importance of a human-centric approach implementation to establish human security. NATO 'The human security approach and guiding principles' embodies this shift focusing on protecting the well-being of humans rather than solely emphasising state security or territorial integrity. Broad-spectrum military or hybrid threats, including armed conflicts, terrorism, and cyber-attacks, as well as propaganda and disinformation, directly affect innocent civilians everywhere in the world. Battlefields are in or among populated areas, unlike the war fronts centuries ago. This shift underscores the need for holistic strategies to protect all individuals by military or non-military means.

As human security encompasses the broader concept of individual welfare rather than solely military might, the human-centric approach serves as a practical tool to achieve human security. Generally, a human-centric approach designs and implements the strategies, systems and policies based on human rights, needs and welfare. The human-centric approach requires more social and emotional intelligence and diversity. Enhanced inclusivity in teams adept at addressing complex security issues is based on various perspectives and specialised expertise. By implementing diverse perspectives and experiences, a human-centric approach can innovate all-encompassing and long-lasting resolutions to security threats, especially those that surpass national and cultural boundaries (Villanueva, 2021). Retired General Michael

X. Garrett suggests a transformation in the army leadership approach and emphasises the importance of inclusivity in the army as a key to team cohesion, directly related to trust, belonging and combat readiness, 'where it matters most: at the point of contact' (Garrett, 2021 p. 1).

Even though the autocratic leadership approach is well-established in military culture, NATO and the EU human security can be seen as a basis for reshaping the traditional leadership paradigms. As is well-known, the autocratic leadership approach minimises followers' involvement in decision-making. Typically, the autocratic leader takes complete individual control over a team and all decisions and rarely accepts advice from followers. This can be true more on a tactical level of leadership; however, on an operational and strategic level, subordinates' diverse perspectives and expertise are well-appreciated; moreover, for instance, sharing recommendations on military response options (MRO) is part of the NATO official planning process (NATO Standardization Office, 2023 pp. 3-66). This suggests that some elements of the feminizations of leadership are implemented in the security sector.

Since the feminization of leadership advocates values and methods that align with transformational leadership, in this chapter, I will discuss the impact and outcome of the feminization of leadership based on research on transformational leadership since researchers have widely studied the latter. Another reason for exploring security outcomes under transformational leadership is that research findings proved that women are transformational leaders.

Previously, I discussed the transformational leadership and approach during peacetime and displayed how positively it affects followers and organisations due to its human-centric approach. This time, I discuss transformational leadership in the security sector in times of crisis, conflict or war. The abovementioned periods threaten safety, security, health and life and are closely related to human stress. In crisis response and mitigation, the role of leaders is incomparably high and vital. This is leadership full talent declaring period.

Transformational leadership correlates positively with followers' well-being and a stress-free environment (Stepanek, et al., 2022). Organisations with a high potential for crisis management can utilise these findings as implementing the transformational

leadership approach can decrease stress levels. Bernard M. Bass and Ronald E. Riggio, in their second edition of 'Transformational Leadership', explored the effect and outcome of transformational leadership through military lenses to address the correlation between stress and transformational leadership.

An effective response is the core endstate to ensure endurance, resistance, peace and stability in the military's complex security challenges. While crisis management is a matter of strategy and tactics, it heavily relies on core elements of leadership, team cohesion and stress management. During a crisis, leaders themselves can cause stress for followers. Those who exhibit only a task-oriented attitude often create a stressful environment, demotivate followers and break team cohesion (Bernard M Bass, 2006 pp. 61-62). On the contrary, team-oriented transformational leaders keep followers motivated, goal-oriented and enthusiastic during a crisis. Transformational leaders bolster a sense of team cohesion and belonging that helps followers not to be paralysed or disbelieved when a crisis arises.

Researchers like Bass and Riggio suggest that teams stay motivated and inspired during a crisis and are more successful under transformational leadership, as leaders are 'concerned but calm, [...] decisive but not impulsive' (Bernard M Bass, 2006 p. 57). Followers show unconditional trust and loyalty to transformational leaders. A leader's dedication and followers' trust enable a leader or commander to ask subordinates to follow and be confident they will, regardless of danger. This level of unity is a crucial aspect in a crisis or war. Team cohesion becomes core in minimising the risks of fear, frustration or mental disorders in the military. By applying emotional intelligence, transformational leaders help minimise the stress level (Bernard M Bass, 2006 pp. 61-62).

The inner strength and fortitude of the transformational leader are also expressed in the fact that they ideally manage their inner stress. For example, Mahatma Gandhi, Charles de Gaulle and Ronald Reagan managed not to lose their sense of humour even when their lives were in danger (Bernard M Bass, 2006 p. 67). High confidence and courage make leaders role models, inspiring and motivating followers.

Integrating women in security, with their distinctive mission-critical perspectives, has generated significant advancements in threat evaluations, leading to more

sophisticated and all-encompassing security strategies. As more women become part of terrorism, more women's perspectives are needed to challenge their effectiveness (Bigio, 2018). Furthermore, a notable correlation is shown between women's presence in decision-making roles and enhanced intelligence capabilities. The pivotal role of CIA female officers in locating Al-Qaeda's founder, Osama Bin Laden, is evidence of how women 'bring their talents, skills, and abilities to advance the intelligence capability' (Martin, 2015 p. 109).

Women leaders often exhibit a blend of assertiveness and empathy, skillfully incorporating resolute measures with a dedication to ethical concerns and long-term strategic foresight. Ensuring stability is paramount within the national security domain, given the substantial and wide-ranging ramifications that decisions in this area entail.

However, the historical influence of women leaders on peace and security is evident. 'Belfast Agreement (Good Friday)' is a decent example of a women's leadership approach to peace and security. In 1998, women in Northern Ireland came together and created a cross-community to push for peace. The Northern Ireland Women's Coalition (NIWC) applied social and ethical dimensions, called for inclusion and diversity, and reached out to marginalised groups to ensure they were heard. Consultations led to the peace agreement (Bramble, et al., 2018). Similarly, the second Liberian civil war (1999-2003) was marked by women's led to a long-lasting peace agreement in conflict resolution. Women established a united support network and, as community leaders, took a mediator role between fighting sides. Peace talks ended with a peace agreement (Zanker, 2018). Moreover, the Falklands War is another prominent example of woman leadership. Margaret Thatcher, in 1982, maintained decisive and strategically vigilant leadership to defend the island and its people and led the United Kingdom to victory (Bruni, 2018 pp. 135-157).

The impact of women occupying leadership roles in national security extends beyond short-term tactical advantages and encompasses broader organisational cultural changes. Including women in leadership roles is a noteworthy indicator and catalyst for instigating progressive organisational changes. This transition entails a departure from previous leadership practices and a return to principles of ethical behaviour, transparency and responsibility, all of which are indispensable qualities in national security.

As a critic, it is imperative to recognise the similarities between male and female leaders, specifically regarding their capacity to adapt their leadership approaches according to the circumstances. Women, akin to men, can exhibit directive and task-oriented leadership styles when the circumstance demands it. Bass notes that sometimes female leaders adopt masculine traits and approaches in male-dominated environments (Bernard M Bass, 2006 p. 113).

Margaret Thatcher and Helen Clark are notably influential figures who question whether there is a difference between men and women in leadership (Simms, 2008 pp. 275-283). This can be the fruit of the thought that women and men may be similar. However, culture, traditions and bias can affect their behaviour. In addition, the constant emphasis on women's empathy and feminine approach to leadership may reproduce cultural norms and gender roles, which exclude women from leadership.

Feminization as a process is an unstable concept that is constantly changing according to time, location, and culture. Understanding feminization is not clear as it describes different processes in different cultures. Furthermore, femininity is neither an innate nor an objective quality; it is a culturally constructed role. As Judith Butler argues, femininity is the reproduction of individuals' assertion that they belong to a particular group (Imhoff, 2016 p. 127).

Conclusion and Recommendations

From a perspective of transforming a task-oriented leadership approach to a more human-centric one, the feminisation of leadership aligns with NATO and EU human security resolutions. This leadership centres on the values of human security, echoing the importance of the human-centric approach and involving a holistic reevaluation of what effective leadership looks like. Alternatively, the rising number of women leaders demonstrates an inclusive culture in organisations; broader, it complements UNSCR 1325 'Women, peace and security.' The resolution affirms that embracing a feminine approach to security and leadership is essential for efficiently tackling contemporary security issues. It introduces diverse perspectives crucial for effectively addressing intricate and multifaceted security issues.

Diverse viewpoints enhance the depth of understanding regarding global security issues' complex, multifaceted nature, thereby promoting the development of more effective and nuanced strategies. The practical ramifications of these diverse viewpoints extend beyond purely theoretical considerations. This demonstrates a commitment to equity and impartiality, critical for forming and sustaining a stable and secure society. As a result, this phenomenon fosters serenity and stability at both the domestic and international levels through innovative thinking and successful problem-solving, which is critical in national security's dynamic and unpredictable realm (Chowdhury, 2021). Proposed by women leaders, the formation of inclusive and nonhegemonic teams is vital to the efficiency and cohesion of a security system. This approach reduces internal tensions and enhances overall performance to deter external threats. Collaborative efforts increase effectiveness between and within national or international agencies.

Considering the evidence, I recommend that the military embrace transformational leadership to enhance the effectiveness of the human-centric approach. The advancement of women leaders within its ranks is another recommendation for gender equality and strategic imperative. Commanders should ensure that there are diverse group and gender advisers, especially on operational and strategic levels, including women.

Feminization in leadership positions about national security signifies a substantial and paradigm-shifting progression, as it facilitates the incorporation of a variety of valued perspectives, encourages the practice of ethical decision-making, and cultivates productive team dynamics. Female leaders contribute substantially by offering unique viewpoints and approaches, fostering inclusive and innovative environments critical for efficiently tackling complex global security challenges. It strengthens national security strategies through alignment with the diverse communities they aim to protect, thus augmenting their flexibility and efficacy. The shift towards a more gender-balanced leadership environment represents progress towards equality and provides a strategic advantage in promoting global stability and peace, responding to human rights and gender equality.

Bibliography

Alice H. Eagly, Linda L. Carli. 2003. The female leadership advantage: An evaluation of the evidence. *The Leadership Quarterly*. December 2003, 14, pp. 807-834.

Alice H. Eagly, Mona G. Makhijani, Bruce G. Klonsky. 1992. Gender and the evaluation of leaders: A meta-analysis. *Psychological Bulletin*. [Online] 1992. [Cited: March 2, 2024.] chrome-extension://efaidnbmnnnibpcajpcgiclfindmkaj/https://mlkrook.org/pdf/Eagly_1992.pdf

Arostegui, Julie L. 2015. Gender and the Security Sector: Towards a More Secure Future. *Connections*. 2015, Vol. 14, 3, pp. 7-30.

Bernard M Bass, Ronald E. Riggio. 2006. *Transformational Leadership*. London : Lawrence Erlbaum Associates, Publishers, 2006. ISBN 0-8058-4761-8.

Bigio, Jammie. 2018. Women's Contributions to Countering Terrorism and Violent Extremism. *Council on Foreign Relations*. February 27, 2018.

Billing, Yvonne Due and Alvesson, Mats. 2000. Questioning the Notion of Feminine Leadership: A Critical Perspective on the Gender Labelling of Leadership. *Gender, Work and Organization*. [Online] December 16, 2000. [Cited: October 24, 2023.] chrome-extension://efaidnbmnnnibpcajpcgiclfindmkaj/https://e-learning.tsu.ge/pluginfile.php/344052/mod_resource/content/1/Week%2011-13%20Part%202%20notion%20feminine%20leadership.pdf.

Bramble, Alexander and Freuler, Nino. 2018. Women in Peace & Transition Processes. Northern Ireland (1996–1998). *Inclusive Peace*. [Online] December 2018. [Cited: 9 December 2023.] <chrome-extension://efaidnbmnnnibpcajpcgiclfindmkaj/https://www.inclusivepeace.org/wp-content/uploads/2021/05/case-study-women-northern-ireland-1996-1998-en.pdf>.

Brenner, O.C., Tomkiewicz, Jozeph and Shein, Virginia Ellen. 1989. The relationship between sex role stereotypes and requisite management characteristics Revisited. *Academy of Management Journal*. 1989, Vol. 32, 3, pp. 662-669.

Bruni, Domenico Maria. 2018. A leader at war: Margaret Thatcher and the Falklands Crisis of 1982. *OpenEdition Journals*. 2018, Vol. 20, pp. 135-157.

Calhoun, Craig, et al. 2007. Classical Sociological Theory. *Internet Archive*. [Online] 2007. [Cited: April 27, 2024.] <chrome-extension://efaidnbmnnnibpcajpcgiclfindmkaj/https://dn790004.ca.archive.org/0/items/ClassicalSociologicalTheoryCraigCalhounJosephGerteisJamesMoodySteveUploadByUni/Classical%20Sociological%20Theory%20Craig%20Calhoun%2CJoseph%2CGerteis%20James%2CM>.

Carlyle, Thomas. 1906. *On Heroes, Hero-Worship & the Heroic in History. Six lectures.* [ed.] Henry David Gray. New York : Longmans, Green and CO, 1906.

Chandler, Diane. 2011. What Women Bring to the Exercise of Leadership. *Journal of Strategic Leadership*. 2011, Vol. 3, 2.

Chowdhury, Anwarul K. 2021. *UNSCR 1325 on Women Peace and Security: Assessment and Recommendations.* [interv.] Saira Yamin. s.l. : DKI APCSS Security Nexus, February 12, 2021.

Fondas, Nanette. 1997. Feminization Unveiled: Management Qualities in Contemporary Writings. *The Academy of Management Review*. January 1997, Vol. 22, 1, pp. 257-282.

Garrett, Gen. Michael X. 2021. Military Diversity. A Key American Strategic Asset. *Army University Press*. [Online] May-Jun 2021. [Cited: April 21, 2024.] <chrome-extension://efaidnbmnnnibpcajpcgiclfindmkaj/https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/MJ-21/Garrett-Military-Diversity-1.pdf>.

Gorska, Anna. 2016. Gender Differences in Leadership. *Studia i Materiały*. January 01, 2016, pp. 136-144.

Imhoff, Sarah. 2016. The Myth of American Jewish Feminization. *Jewish Social Studies: History, Culture, Society* . 2016, Vol. 21, 3, pp. 126-152.

Khan, Zakeer Ahmed, Khan, Irfan Ullah and Nawaz, Allah. 2016. Leadership Theories and Styles: A Literature Review. *Researchgate*. [Online] February 11, 2016. [Cited: November 22, 2023.] chrome-extension://efaidnbmnnnibpcajpcgiclfindmkaj/https://www.researchgate.net/profile/Allah-Nawaz-2/publication/293885908_Leadership_Theories_and_Styles_A_Literature_Review/links/56bcd3ad08ae9ca20a4cdea2/Leadership-Theories-and-Styles-A-Literature-Review.pdf. ISSN 2422-8397.

Martin, Amy J. 2015. America's Evolution of Women and Their Roles in the Intelligence Community. *Journal of Strategic Security*. 2015, Vol. 8, 3, pp. 99-109.

NATO Standardization Office. 2022. *AJP-3.2 Allied Joint Doctrine for Land Operations*. B, version 1. s.l. : NATO Standardization Office (NSO), 2022. pp. 42-43.

—. **2023.** *Comprehensive Operations Planning Directive*. Mons : NATO Standardization Office (NSO), 2023. p. 501.

North Atlantic Treaty Organization (NATO). 2022. Human Security. *North Atlantic Treaty Organization*. [Online] 2022. [Cited: December 13, 2024.] https://www.nato.int/cps/en/natohq/official_texts_208515.htm?selectedLocale=en.

Passer, Michael W. and Smith, Ronald E. 2007. *Psychology. The science of mind and behaviour*. 4th. New York : McGraw-Hill Humanities, 2007. ISBN-13: 978-0-07-338276-0 ISBN-10: 0-07-338276-0 .

Sayeed, Omar Bin and Shanker, Meera. 2009. Emotionally Intelligent Managers & Transformational Leadership Styles. *Shri Ram Centre for Industrial Relations and Human Resources*. April 2009, Vol. 44, 4, pp. 593-610.

Simms, Marian. 2008. Are Women Leaders Different? Margaret Thatcher and Helen Clark. [book auth.] Paul 't Hart and John Uhr. *Public Leadership. Perspectives and Practices*. s.l. : ANU Press, 2008, pp. 275-283.

Stepanek, Sarah and Paul, Megan. 2022. Umbrella Summary: Transformational Leadership. *QIC-WD Quality Improvement Center For Workforce Development*. [Online] Jul 13, 2022. [Cited: February 24, 2024.] chrome-extension://efaidnbmnnnibpcajpcgclcfindmkaj/https://www.qic-wd.org/sites/default/files/Umbrella%20Summary%20-%20Transformational%20Leadership%20071122.pdf.

Stogdill, Ralph M. 1974. *Handbook of leadership: A survey of theory and research*. New York : The Free Press, 1974.

Suciu, Marta – Christina, Bocaneala, Ana – Maria and Dumitresku, Decebal Octavian. 2023. The Women Leadership. A Human-Centered Approach. *Sciendo*. [Online] July 14, 2023. [Cited: February 4, 2024.] chrome-extension://efaidnbmnnnibpcajpcgclcfindmkaj/https://intapi.sciendo.com/pdf/10.2478/picbe-2023-0150#:~:text=Women's%20leadership%20involves%20certain%20qualities,an%20in spiring%20leadership%20role%20model..

United Nations General Assembly (UNGA). 2012. *General Assembly of the United Nations*. [Online] October 25, 2012. [Cited: November 24, 2023.] chrome-extension://efaidnbmnnnibpcajpcgclcfindmkaj/https://www.un.org/humansecurity/wp-content/uploads/2022/06/N1147622.pdf.

—. 2005. Welcome to the United Nations. *United Nations*. [Online] October 24, 2005. [Cited: April 24, 2024.] chrome-extension://efaidnbmnnnibpcajpcgclcfindmkaj/https://www.un.org/en/development/desa/population/migration/generalassembly/docs/globalcompact/A_RES_60_1.pdf.

United Nations Security Council (UNSC). 2000. Res 1325. *United Nations Peacekeeper*. [Online] octomber 31, 2000. [Cited: November 24, 2023.] chrome-extension://efaidnbmnnnibpcajpcgclcfindmkaj/https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/WPS%20SRES1325%20.pdf.

Van Engen, M.L. 2001. *Gender and leadership: A contextual perspective*. s.l. : Tilburg University, 2001.

Villanueva, Danielle. 2021. Operationalizing Women, Peace, and Security in the Armed Services: Army Strategic Implementation Plan. *Defence Technical Information Center*. [Online] April 27, 2021. [Cited: April 11, 2024.] chrome-extension://efaidnbmnnnibpcajpcgclcfindmkaj/https://apps.dtic.mil/sti/trecms/pdf/AD1178343.pdf.

Yukl, Gary A. 2006. *Leadership in Organizations*. [ed.] Sally Yagan. 8th . Boston : Pearson, 2006. p. 528. ISBN 10 0132771861.

Zanker, Franzisca. 2018. Women in Peace and Transition Processes: Liberia (2003–2011). *Inclusive Peace*. [Online] April 2018. [Cited: December 9, 2023.] chrome-

extension://efaidnbmnnnibpcajpcgicfindmkaj/https://www.inclusivepeace.org/wp-content/uploads/2021/05/case-study-women-liberia-2003-2011-en.pdf.

Zannat, Mahfuza, Longhai, Zhang and Forkan, Sanjida. 2020. A Comparative Study Between Plato and Aristotele's Philosophy. *An International Peer Reviewed Refereed Journal*. August 2020, Vol. 1, 3, pp. 39-46.

KAURI RAJU. What are the organisational outcomes from the relationship and the implications between leadership, management, and command?

Introduction

John Calvin Maxwell, an American author who has written many books about leadership and has sold millions of copies of those, has said, 'The pessimist complains about the wind. The optimist expects it to change. The leader adjusts the sails' (Maxwell, n.d). The previous quote gives a brief but concise idea of leading people. Just as the weather can change, so can the environment, affecting organisations at different levels and in different sectors of activity. To be effective, a leader needs to be able to adapt quickly to the changes that occur. It is common knowledge that, in recent years, Western society has been confronted with various challenges and problems. Examples include the SARS-CoV-2 coronavirus pandemic affecting the entire world, an unstable financial and economic environment, and an energy security or migration crisis primarily affecting Europe. Responding to these complex situations and challenges requires competent leaders in all areas and levels of governance.

A similar situation exists in the military. Many of the significant societal changes also influence how military structures function and are led. Furthermore, due to the ongoing war in Ukraine, the security environment for Western countries has become uncertain and unpredictable. So, this raises the question of what kind of leader is most appropriate for the military in a complex and rapidly changing environment. Given the inherent unpredictability, disorder, randomness, and resistance encountered in military leadership, adjusting to the circumstances and identifying appropriate strategies and approaches is crucial. To find the organisational outcomes, this study uses three specific terms to describe governance in Western military structures. These terms are leadership, management, and command (hereafter abbreviated as LMC). Designated terms have been selected because they may offer distinct perspectives individually, but when used in conjunction, they might provide a comprehensive picture of governance within a military organisation. These phrases are frequently used independently in discussions on governance, although some may argue that this approach fails to provide a comprehensive understanding. Furthermore, the relationship and implications between these three terms could provide insight into critical organizational outcomes.

To achieve a clear and precise comprehension of LMC terms, it is necessary to have a definition that explicitly presents an explanation and aids in gaining an understanding of the underlying concept. However, locating the universally accepted definition can be challenging despite the vast number of books, papers, and articles on leadership and management in the civic literature. Given that the paper focuses on governance methods in a military organization, it could be meaningful to use official field-specific terminology. Thus, this study uses official NATO or its member and partner state definitions as the foundation for understanding leadership, management, and command concepts and presenting a comprehensive understanding of their interconnections.

So, this research paper argues that the greatest benefits to the military organisation are when leadership, management, and command are used in combination rather than in isolation.

This paper will be divided into five chapters to support the argument. The first three chapters concern the official definitions, explanations, and concepts of leadership, management, and command, which provide the necessary background knowledge. The fourth chapter provides an overview of similarities, differences, and the relationship between LMC. The fifth chapter discusses the relationship and applicability of the first four chapters' results in military organizations.

Command

NATO glossary of terms and definitions gives five different explanations for the term command. The most appropriate definition in the context of this study can be considered to be as follows - 'The authority vested in a member of the armed forces for the direction, coordination, and control of military forces' (NATO Standardization Office, 2021 p. 29). To fully understand the given explanation about command, the meaning of authority requires additional clarification. The Oxford English Dictionary defines authority as 'the power or right to give orders and enforce obedience' (2006 p. 88). In the current context, it can be interpreted that a member of the armed forces with vested authority is permitted to exert control over others, and the designated authority grants legitimacy to this influence.

The definition itself does not give a direct answer to the question of who vests the authority. However, in the military organisation, every commander has his or her superior from the lowest level of the structure to the very top. So, it is crucial to emphasise that the military's hierarchical framework distinctly establishes the chain of command and the subordination of individuals. Therefore, both the military rank and the position establish the hierarchy and authority to direct, coordinate, and control only designated military forces. A simplified explanation would be that the delegator of authority can be superior to a subordinate according to the chain of subordination. But a more substantive explanation is that every national military system is heavily regulated and covered by the legislation. For example, in the UK Joint Operations Doctrine, it is stated that 'It has a legal and constitutional status – codified in Queen's Regulations. It is also vested in a commander by their superior' (2014 p. 101). So, a concise answer to the question of who could be superior with legal status is vested by law.

Nevertheless, it is crucial to comprehend that the privilege of command entails more than just the lawful entitlement to exert influence over others. It should be acknowledged that authority also carries the burden of responsibility and the obligation to be accountable. The same legal basis that gives the right to command others also sets the rules for accountability. In the army, there is an old saying that the commander has full responsibility for all actions or omissions of the unit. Australian officer, Colonel Michael Scott, has stated that a soldier, sailor, or airman is personally responsible and answerable for their actions, behaviour, and performance at all times. However, for commissioned or non-commissioned officers, the notions of responsibility and accountability extend beyond individual actions to encompass the combined actions, behaviour, performance, and outcomes of the organisation that the officer leads or supervises (Scott, 2021).

Since the command definition used above does not provide a clear and straightforward explanation of the necessity for command, it is important to briefly address this issue to achieve a thorough comprehension. The explanation addresses the concepts of guiding, coordination, and control, but it fails to clarify the ultimate objective. It can be considered as a common knowledge, that the military environment can be stressful and dangerous. Hence, military commanders must possess the capability to retain

command over their subordinates and effectively execute the prescribed assignments, even in the most challenging circumstances. A command can be seen as the act of leading individuals in a manner that facilitates the accomplishment of the assigned task. So, the necessity for command can be considered to be the fulfilment of an objective or a goal and control, coordination and guidance are the means to achieve them.

In essence, the command is composed of assigned rights and responsibilities vested in a member of the armed forces who, through activities directed at military personnel aims to achieve collective objectives with having a conceptual character based on legality. However, understanding the meaning of command is merely one aspect of comprehending the governance of individuals or groups in a military organisation, which does not provide a comprehensive perspective. The next chapter will therefore focus on the concept of leadership in more detail.

Leadership

It has been argued that despite substantial research on leadership, it remains one of the most intricate and multifaceted phenomena, leading to ongoing and perplexing debates due to its inherent complexity (Benmira, et al., 2021). Just as academics have disagreed on a single definition of leadership, there is no explanation about leadership in the NATO glossary of terms and definitions (NATO Standardization Office, 2021). However, the chronicles of human history are littered with famous people who held leadership roles, ranging from influential heads of state to invincible military commanders. Nevertheless, the notion of leadership remains a subject of ongoing discourse and scholarly investigation, as individuals strive to comprehend the essence of true leadership. Even if it may be challenging to quantify the importance of the military's influence in shaping the principles of leadership, the military has certainly played an essential role in it through the ages, and nowadays, the principles of military leadership are based on general principles of leadership. While NATO lacks a commonly established definition of leadership, individual armies typically establish their own definitions that serve as a foundation. For example, the United Kingdom (UK) Army Leadership Doctrine states the definition of leadership as follows - 'A combination of character, knowledge and action that inspires others to succeed' (n.d pp. 1-2). At the same time, the doctrine of the United States (U.S.) Army states that 'Leadership is

the activity of influencing people by providing purpose, direction, and motivation to accomplish the mission and improve the organization' (2019 pp. 1-3).

To ensure a better understanding of the concept of leadership, a combined analysis of both definitions is used. The UK version emphasises action combined with character and knowledge, whereas the U.S. version specifically highlights motivation and the provision of direction and purpose as an action. Furthermore, both interpretations encompass also endeavours directed towards exerting influence on others to attain an objective. As mentioned above, from both definitions it is possible to identify the actions through which, in the first case, the aim is to inspire people and, in the second case, to influence them. Even if the actions and methods of influencing others are worded differently, their purpose is the same. Therefore, it can be argued that influencing is an essential part of leadership aimed at achieving the desired objective. So, both explanations also reflect the goals that these activities are intended to achieve. In the first case, the goal is success and in the second, mission accomplishment and organisational improvement. However, it can be argued that these different formulations also contain the same meaning, because fulfilling a mission can be equated with success and vice versa. Again, it can be said that, despite the difference in wording, the objective reflected in both definitions is the same.

Both definitions embrace the presence of the governed party. So that the goal can be achieved the leadership necessitates the presence of two interconnected components: the leader and the people they lead. Even if leadership in the military can be considered a task assigned to commanders, the definitions under discussion do not refer specifically to any leaders. It can be argued that every member of the Army should possess a fundamental comprehension of the nature and functions of leadership as it helps to maximize the result of leadership in the organisation. If all members of the organisation understand the principles in the same way, they will understand the role of their superiors and be able to contribute to it.

Comparing these two definitions, it can be said that, despite the difference in wording, the basic concept is similar. In principle, the distinction lies only in the level of detail of the different components of the concept that are to be emphasised. However, both definitions include different activities aimed at influencing people to achieve success.

Previous definition explanations about leadership also prove the earlier statement that the principles of military leadership are based on general principles of leadership. This can be demonstrated by employing Peter G. Northouse's leadership definition components. According to his framework, leadership is characterised by a process and an influence that occurs inside groups and encompasses a shared objective (2013 p. 5) and all these components are also identifiable in the previously used definitions of leadership.

To briefly summarise the previous chapter, it can be said that leadership is characterised by the variety of actions of one party to influence others to achieve objectives. It is important to stress that people are an essential part of leadership. If there are no people to influence, then the various means of influence and actions will be of no use and the objective will not be achieved. But is it only the person who is important in governance, or can other resources also be important?

Management

It has been stated that in U.S. Army doctrine and also in practice there is no distinction between leadership and management and the differences between the two concepts are blurred (Gallagher, 2016). Furthermore, even in the NATO glossary of terms and definitions, there are several different definitions which include management, but none of them provides a precise explanation of the concept of management itself. Most of the definitions that include management relate to different resources or processes. Examples include risk management and supply management or crisis management with explanations involving various activities (NATO Standardization Office, 2021 pp. 36, 72, 113). However, official definitions can be found in the doctrines of some other countries. For example, in the Australian Army Land Warfare Doctrine management definition is stated as follows 'The process of planning, organising, directing and controlling organisational resources in the pursuit of organisational goals' (2003 pp. 1-7). In the UK Army Leadership Doctrine is the concept of management described as the methods, processes, and techniques for controlling and distributing resources, such as personnel, equipment, financial resources and more. It employs organisational structures and processes to mitigate risk and deliver optimal results with maximum efficiency (n.d pp. 1-5). So, both sources are used to analyse the concept of management and to understand its concept. As the first similarity, both formulations include a process, which refers to an ongoing activity. This, in turn, can be interpreted

to mean that the precondition for the functioning of management is to ensure that activities are continuous. Another similarity can be found in the activities that are part of the process mentioned above. Australian definition refers to controlling, directing, planning, and organising as the UK version mentions control and allocation of resources. Thirdly, both wordings refer to resources. The first example refers to the organization's resources in a generic manner, while the second case specifically identifies financial resources, human resources, and material resources. The last common feature is the goal. Again, the Australian version refers broadly to the organisation's objectives, while the UK version describes the ultimate aim as mitigating risk and achieving the optimal outcome with maximum efficiency.

Similarly to the leadership section, even if the wording and level of detail may vary, the fundamental concepts of the management definitions remain comparable.

Based on the preceding information, one can say that the most crucial aspect of management is having a diverse range of resources, which defines it as a way of governance.

Similarities, differences, and the relationship between LMC

Now that the first three chapters have clarified the LMC concepts through definitions and the background knowledge has been created, it is possible to address the comparisons, contrasts and interrelationships of these terms within the military organisation. It is crucial to remember that the military's hierarchical structure specifies the chain of command and the subordination of individuals. Furthermore, the contention can be made that the principles mentioned above serve as the foundation for the military definitions employed in the paper, as they originated from authoritative manuals or doctrines. In summary, the above can also be considered as a relationship where the military organization has shaped the definitions used in it, and the definitions reflect the organization's needs and characteristics.

As the first step, comparisons of similarities and differences between the components of the concepts are used to examine the relationships between LMC. So, all three concepts share the similarity of involving two parties. One party is the implementer of the command, leadership, or management, and the other party is the actor to whom

they are applied. Since it is about governance methods, it can also be argued that, in most cases, the relationship is between subordinate and superior, with the superior being the LMC implementer. Yet there is also a difference between the parties. While command and leadership are about interpersonal processes, management involves not only human resources but also, for example, material and financial resources. While the implementation of command and leadership may require the employment of some material components, it is important to note that it cannot be regarded as a distinct purpose according to its definition. On this basis, it can be argued that those servants who are involved in management also might need the knowledge and skills to deal with resources other than people. Furthermore, this can be considered one of the important aspects to be taken into account by the organisation.

Another similarity is that in all LMC concepts, one of the elements is the factors or activities. For example, command refers to authority, direction, coordination, and control; leadership refers to influencing or inspiring people; and management refers to the process of planning, organising, directing, and controlling. These actions and causes also emphasise the distinctions that define each governance method. A command is distinguished by its authoritative nature, which indicates its legitimacy. Leadership involves the act of influencing others, while management is marked by an organised process comprising multiple actions. Thus, the activities or factors are similar only because they are components of the LMC definitions, and the activities presented are rather different. However, it is the distinctions that allow the essence of each concept to be identified and determine its applicability in an organisation. Highlighting this distinction provides an opportunity to move on to more substantive issues.

The final commonality of all LMC principles that will be highlighted is the goal or outcome. Through the investigation of the definitions presented in the preceding chapters, one can also observe a manifestation of the goals embedded inside these definitions. Within the concepts of leadership and management, one might discover a formulation that explicitly mirrors the organisational objectives. Even if the wording of the definition of a command does not reflect the final objective, the analysis nevertheless identifies it. To have a deeper comprehension of the correlation between LMC goals inside the organisation, it is imperative to establish a connection between the organisation and the definitions provided in the initial paragraph of this chapter.

From these relationships, it can be deduced that the goals inserted in the terms discussed are closely linked in one way or another to the goals of the organisation.

Since comparisons of conceptual components can be considered relatively technical and provide only partial clues to organisational outcomes, the following section focuses on the possible hierarchy of the LMC concepts within a military organisation.

One possible option is to view a command as a comprehensive approach that encompasses both leadership and management. As stated in the first chapter, a command is characterised by the legal right to exert control over others, and this right is vested in a member of the armed forces by the military organisation and the legislation. It is also known that the military organisation has a hierarchical structure, with a clear relationship of subordination. Thus, it can be argued that since leadership and management are subject to the same regulations in the same system, implementing them both also requires a juridical right. It also can be said that effective leadership of a unit or management of materials, finances, or other resources requires having vested authority as they both can be considered as positional powers in structural hierarchy. Furthermore, in the Australian Army Land Warfare Doctrine is stated that the command grants the lawful power and accountability to accomplish a task, and leadership and management are the two methods by which the task is fulfilled (2003 pp. 1-8). So, from an organisational point of view, it can be said that the command creates the conditions for the implementation of leadership and/or management. Additionally, there is no indication of a hierarchical distinction between leadership and management, as both can be equally and appropriately executed.

Notwithstanding the foregoing, it is possible to find references that treat the LMC hierarchy differently. One hint can be found in Charles R. Gallagher's approach, which defines personal power as a component of leadership that extends beyond the authority granted by command (2016).

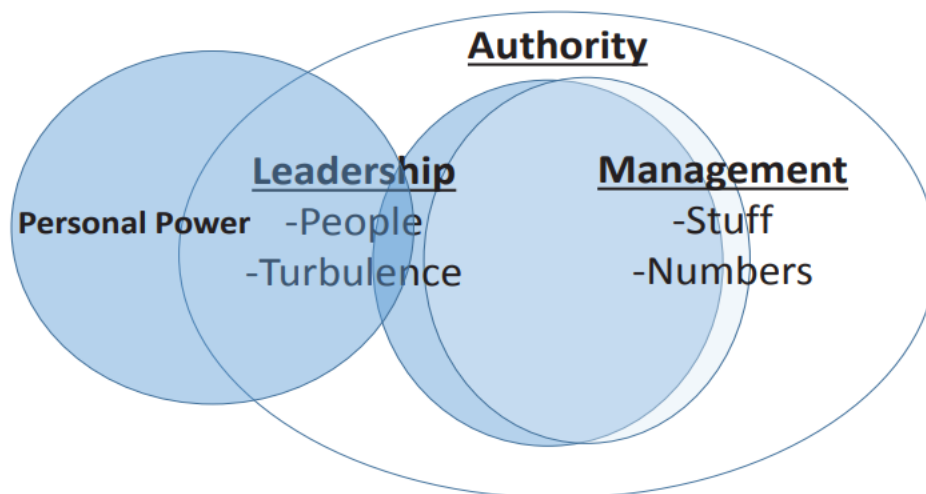


Figure 1. Leadership beyond Command

Source: Adapted from (Gallagher, 2016)

Figure 1 indicates that leadership and management overlap under authority, but personal power is partially stretched out of the circle. Therefore, leadership does not solely depend on authority provided by command, and a portion of it can be exercised without legal entitlement. The foregoing is supported by the definitions of leadership analysed in chapter two since there is also no limitation to the use of leadership only by an authorised superior. So, it can be argued that every member of the military can implement leadership to some extent. To illustrate such a scenario, an example can be given where a designated leader is not present and a soldier without formal authority encourages others to carry out an assigned task. Even if, in such a situation, the soldier has no legal right to influence others, and others are under no obligation to obey, it is feasible and aimed at achieving the objective. In light of the foregoing, it can be argued that leadership can be considered more important than command in certain situations, as it can be exercised by military personnel without legal authority in order to achieve the assigned goals.

As a final example, a completely different approach is used to describe a possible LMC hierarchy. This convergence is not related to the formal definitions used in the work, but it has been used to interpret the LMC relationship in an organisation and provides an alternative point of view to the topic. So, some scholars use the complexity of problems to describe and compare command, leadership, and management. In Keith Grind's approach, the command is linked to Critical Problems characterised by the authoritarianism of the commander, without uncertainty in the actions expected from the leader, and limited time for decision-making and action. Management is related to

Tame Problems, defined by a limited degree of uncertainty and the resolution of problems already experienced. Tame problems are comparable to puzzles, for which there is always a solution that can be achieved using a standardised operating procedure. Leadership is related to Wicked Problems, encompassing a combination of intricate recognised issues and unknown problems. It involves a significant degree of uncertainty, necessitating a group effort rather than an individualistic one (2008 pp. 11-12).

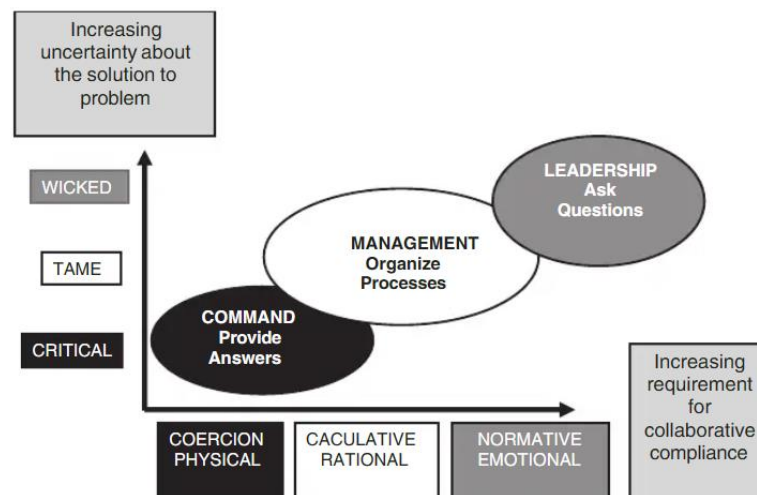


Figure 2. Typology of problems, power and authority

Source: (Grint, 2008 p. 16)

Figure two can be interpreted as a hierarchy between command, leadership and management as they are treated as an authority in this scheme. The command is considered the lowest due to its reliance only on the acts of the leader and the presence of a clear solution to the problem. Leadership occupies the highest position as it necessitates the participation of several actors, while also being characterised by a significant degree of uncertainty. Management, on the other hand, falls in between these two levels, with some degree of overlap and similarities with both.

In summary, this chapter highlights the importance of understanding the similarities, differences, and potential hierarchies in order to comprehend the interconnections among LMC. In addition, the above information provides the basis for a better understanding of organisational outcomes.

Applicability of LMC in military organisation

After analysing the definitions and concepts and determining their similarities, differences, and potential hierarchy, it is now feasible to accurately determine the organisational outcomes. By now, it has also been proven that while LMC are all governance methods, they should not be considered synonymous. Even if they all have similarities, which are also highlighted in this work, it can be argued that it is the differences that determine their importance for the organisation.

It is stated that the art of command is unique to the military (Headquarters Training Command – Army, 2003 pp. 1-7). In military organisations, the command provides the legal right to direct and control others to those who are authorised to do so through rank, position, and formal hierarchy. It can be argued that military structure, which deals with constant threats and changes, requires a clearly regulated chain of authority and system of command, and without legal entitlement, those could be hard or even impossible to achieve. Simultaneously, it might be contended that, inside a military organisation, mere adherence to legal authority is insufficient, necessitating the implementation of other approaches to facilitate the attainment of the desired outcome. Now it is relevant to highlight again the previously mentioned Australian principle, which states that leadership and management serve as a tool to achieve a goal (Headquarters Training Command – Army, 2003 pp. 1-8). Consequently, it may be inferred that a military organisation requires legal authorization to establish a hierarchical structure but that other methods are also needed to support the achievement of the organisation's objectives.

Chapter Two elucidated that leadership is distinguished by the ability to exert influence and inspire others. As discussed above, leadership can be based on a legal authority or, in some cases, without one. Superiors apply it according to subordination and others are subordinate to it. Without the right of command, soldiers can also influence their comrades. In both cases, the aim is to accomplish a given task or even to improve the organisation. It can therefore be argued that leadership is necessary for the military organisation as it concerns all the people in it and, through them, enables the achievement of stated goals.

Management is differentiated from leadership and command based on the distinct resources that are being managed. While management shares similarities with leadership and command due to its involvement with human resources and the requirement of legal power, it is a distinct and significant component of overall governance. Therefore, it can be asserted that management is essential for the operation of a military organisation, as it involves the efficient utilisation of diverse resources, ranging from weaponry to financial assets. Thus, management plays a crucial role in attaining organisational objectives since it adds governance outputs that are distinct from those provided by command and leadership.

The previous discussion addressed each outcome of LMC for the organisation separately but also revealed a close interconnection with the other methods under consideration. However, the next analysis examines them collectively. It also examines whether the combination of LMC is more advantageous for a military organisation than using them in isolation. So, based on the preceding chapters, it is evident that LMCs exhibit several signs of shared elements and intersections, which are present in both the definition's components and the potential hierarchy. For instance, each of the three methods functions between two parties, to achieve a task, and there may exist varying hierarchies among them. So, it can therefore be argued that similarities create overlaps between LMCs, which can be considered an important prerequisite for their use together. An illustrative example of this is a scenario in which a military commander is granted the legal authority to influence their subordinates while simultaneously overseeing the allocation of essential resources. Each of the three, is represented by its specific features, which complement the others and create flexible options for the leader. Moreover, the aforementioned evidence corroborates the fact that several armies treat LMC as a combination. For example, the Australian Army Land Warfare Doctrine, cited earlier in this work, can be taken as an example. This doctrine is aimed at leaders at different levels and is intended to provide a framework for understanding the nature of governance in its future application (2003 p. 9). This unequivocally demonstrates that the principles of LMC are mutually reinforcing and indispensable for leaders to make meaningful contributions towards accomplishing the organization's goals in a swiftly evolving environment.

In the light of the foregoing, it is difficult to find evidence that command, leadership or management would be more effective for an organisation in isolation than in

combination. It can be said that command in isolation is of no use because, without a led workforce and other resources, tasks cannot be performed. The military system requires a legal basis, provided by the command. However, as identified earlier, leadership can also operate without the right of command through personal power, but this can be only a temporary solution. Such situations may be seen as beneficial to the organisation but are not sustainable in a system with fixed subordination. Therefore, it can be argued that leadership needs a command to operate effectively within the established chain of command. The same is the case for the management of resources, which requires a legal basis. It is not possible to have access to the exploitation of military resources without a designated authorisation. So, this chapter's conclusion is that, even if command, leadership and management can be considered separate methods of governance, the foregoing proves that the best way to achieve organisational objectives is to use them in combination.

It is now fitting to revisit the John Calvin Maxwell quotation cited earlier in the introduction, which discussed the leader's capacity to adapt to the changes in the environment by adjusting the sails. Given the inherent unpredictability, disorder, randomness, and resistance encountered in military governance, it is crucial to adjust to circumstances and identify appropriate resolutions and approaches. Based on the preceding analysis, it can be contended that the integration of LMC equips military commanders with the requisite knowledge and abilities to effectively respond to the dynamic and crucial circumstances that typify a military entity. The command gives the commander legal authority over military troops; leadership adds strategies to influence and/or inspire personnel; and management complements the numerous resource-handling activities. The omission of some methods can significantly reduce the ability to react to different possible situations and therefore the final result will be affected.

On the basis of what has been discussed in the paper, it can be argued that the argument raised at the beginning of the work has been proven. It is important to mention that this conclusion was reached using an analysis of the LMC's official terminology, the similarities and differences identified and the possible hierarchies. So, LMC used in combination provides greater benefits to the military organisation than in isolation. The benefits lie in the similarities between these methods, which reinforce the relationship between them, and even more the differences, which complement the other methods. This combination equips military leaders with the essential knowledge

and adaptability to respond effectively to novel circumstances that may arise in the constantly evolving environment. Furthermore, increased access to diverse ways and means of governance enhances the ability of military leaders to effectively address shifting conditions and accomplish their tasks.

Conclusion and recommendations

There have been many recent events in the world that pose new challenges in different areas of life, including in the military. Leaders are facing increased pressure to handle uncertain situations due to a dynamic and unpredictable environment. This prompts to look into the most suitable methods for military leaders to use. So, this paper aimed to find out whether command, leadership, and management are more useful to an organisation individually or in combination. To determine the answer, three key concepts employed in the armed forces of Western countries were utilised: command, leadership, and management. Some may argue that the utilisation of sources solely from English-speaking countries in the work fails to provide a sufficient comprehension of these terms. However, these countries are all members of a collective of the Western world that possess shared perspectives and customs. This gives rise to the assumption that also perceptions of governance are no different. The initial three chapters focused on the authoritative definitions, elucidations, and principles of command, leadership and management, which furnished the essential foundational understanding. The fourth chapter presents a comprehensive analysis of the parallels, distinctions, and interconnections among LMC. The fifth chapter concludes by examining the correlation and practicality of the findings from the preceding four chapters inside military organisations. The results of the study reveal that LMC offers greater advantages to the organization as an integrated package since it enables military commanders to adapt more readily to changes in a flexible manner. Even if they are all stand-alone terms and methods that have an important role to play in governance, they do not give the same result in isolation as they do in combination.

Considering the results of this paper, it can be recommended that military personnel should always receive an explanation of the LMC concepts at the same time. A coherent approach to LMC can ensure a comprehensive understanding of these terms across the organisation and allow for a deeper insight into their similarities, differences, and relationships. This approach enables leaders to recognise potential areas of weakness in the application of certain governance techniques and to take autonomous

action to address inadequacies. As a result, commanders are better equipped to rapidly recognise the nature of issues in intricate or dynamic scenarios and choose the best LMC combination to accomplish the given goal. As a result, better prerequisites for meeting the organisation's objectives have been created.

Bibliography

Army Doctrine Publication. 2019. Army Leadership And The Profession. *ADP 6-22*. 2019. pp. 1-3.

Benmira, Sihame and Agboola, Moyosolu. 2021. Evolution of leadership theory. *BMJ Leader*. [Online] 2021. [Cited: 11 02 2024.] <https://bmjleader.bmj.com/content/leader/5/1/3.full.pdf>.

Development, Concepts and Doctrine Centre. 2014. UK Joint Operations Doctrine. *Joint Doctrine Publication 01*. November 2014. p. 101.

Gallagher, Charles R. 2016. Muddling Leadership and Management in the United States Army. *Military Review*. August 2016.

Grint, Keith. 2008. *Leadership, management and command: Rethinking D-Day*. 2008.

Headquarters Training Command – Army. 2003. LWD 0-0 Command, Leadership and Management,. *Australian Army, Land Warfare Doctrine*. 2003.

Land Warfare Development Centre. 2017. Army Land Operations. *Army field Manual (AfM)*. 2017. pp. 6-2.

Maxwell, John Calvin. n.d. "John Maxwell Quotes.". [Online] n.d. [Cited: 22 October 2023.] <https://www.quotes.net/quote/39832>.

NATO Standardization Office. 2021. AAP-6. *NATO Glossary of terms and definitions (English and French)*. 2021. p. 29.

Northouse, Peter. G. 2013. *Leadership. Theory and Practice. Sixth Edition*. 2013. p. 5.

Oxford English Dictionary. 2006. *Concise Oxford English Dictionary*. s.l. : Oxford University Press, 2006. p. 88.

Scott, Michael. 2021. Responsibility, Accountability and Culpability – Three Cognitive Pillars to Guide Command Comprehension and Decision Making. *The Cove*. [Online] 22 11 2021. [Cited: 06 12 2023.] <https://cove.army.gov.au/article/responsibility-accountability-and-culpability-three-cognitive-pillars-guide-command-comprehension-and-decision-making>.

The Royal Military Academy Sandhurst. n.d. The Army Leadership Doctrine, UK. n.d.

Marko Saarela. Offensive cyber operations and their impact/influence on National Security.

Introduction

Throughout history, the military has been a tool for the state to secure and achieve political goals. Self-defense has been a basis for all states, and for a long time, it has been enabled mainly by land-, sea- and air forces. Clausewitz and his books are still used heavily in strategies. He wrote, 'War is not merely a political act but a real political instrument, a continuation of political intercourse, a carrying out of the same by other means' (Clausewitz, 1946 p. 280). From this statement, we can conclude that war is the extension of politics by other means. In recent conflicts and wars, cyber has become a more and more critical domain that supports the achievement of required effects and goals.

During the last decades, information communication technology (ICT) has made considerable developments regarding the availability of systems, speed, cost, etc. All this has been pushing states to adopt digital transformation principles. This means that states integrate digital technology into all aspects of their organizations. It involves evaluating an organization's processes, products, operations, and technology stack to identify opportunities for increasing efficiency (McKinsey and Company, 2023). This is one of the factors that has driven the states to develop cyber doctrines and policies to establish defensive and offensive activities as a part of the overall use of the cyber domain. Academics are engaged in conversations regarding the notion that the capabilities for cyber offensive actions should serve as a means of deterrence (Schulze, 2019). Deterrence in cyber usually means two types of effort. Deterrence by denial is less aggressive, and the focus is more on the defensive side to make it clear to an attacker that a possible attempt will not be successful (Iasiello, 2014, p. 55). Deterrence by punishment is more aggressive, the goal is to make sure that the opponent is aware of the significant punishment in retaliation for the attack (Iasiello, 2014 p. 55). From this point, we can conclude that if the nation is talking about deterrence in the cyber domain, it means that the nation owns offensive capabilities.

Many states have had some experiences in the cyber domain in the last decades, and there is an extensive academic discussion over the role of offensive cyber operations in modern military strategies. There is no one-way solution to build up cyber power. According to Muller, states often act differently when talking about cyber, for example, two small countries, Norway and Netherlands, have quite similar understandings of cyber threats. However, their approach to dealing with these topics differs (Muller, 2019 p. 3). Why is it like this? It is all about the state's historical experiences and the available resources, which, in turn, are reflected in strategies (Muller, 2019); (Schulze, 2019 p. 1).

Cyber strategy is a relatively new thing in the states, especially offensive operations, which is why risk is always high in cyber actions. This also explains the main reasons why cyber capability management and decision-making are centralized and, on a high level, very similar to the determination of nuclear weapons use (Lewis, 2015 pp. 7-8). For commanders at all levels, it is always essential to understand the possible effects and how they can mitigate possible risks. One way to lower the risk is to exercise these activities in cyber ranges, where units will be forced to synchronize activities and develop possible tools for real-life use. Lewis also highlights the importance of cooperation and coordination to downgrade the possible risks at different levels (Lewis, 2015 p. 8).

According to the scholar's disputes, I will analyze in this paper different approaches to offensive cyber operations and how these are influencing national security. The research questions that are leading this academic paper are the following:

1. What are the offensive cyber operations?
2. Where can offensive cyber operations be used, and what are the possible effects?
3. What are the risks and challenges of using offensive cyber operations?
4. What are the effects of offensive cyber operations on national security?

This research paper aims to analyze offensive cyber operations within the context of joint force operations and the possible effects on national security. This argumentative essay explains the critical role of offensive cyber operations in modern military strategies, which affects the development and range of warfare and state defense mechanisms. Furthermore, this research explores the transforming nature of offensive

cyber operations and that cyber is not a single warranty for national security. It also brings out the strategic advantages and possible risks while offering actionable recommendations for policymakers and stakeholders to navigate the complexities in the cyber domain effectively.

1.1 What are the offensive cyber operations?

The way how states build up their defense forces has changed a lot. In many states, offensive cyber operations have become increasingly essential to support achieving strategic objectives. In the last decade, offensive cyber operations have extended beyond traditional military objectives and taken a broader role in shaping strategic goals. In this paragraph, I will focus on answering the following questions: What are offensive cyber operations? What are real-life examples based on public resources?

NATO defines an offensive cyber operation as an action in or through cyberspace designed to project power to create effects that align with strategic goals (AJP-3.20, 2020 p. 4). In recent years, one good example of how offensive cyber capabilities can be used is to influence elections and manipulate public opinion. Moreover, in countries like China and Russia, we can identify state-sponsored actors suspected of orchestrating offensive cyber campaigns to influence political outcomes in other states by circulating disinformation and exploiting vulnerabilities in an electoral system (Austin, et al., 2022).

Additionally, since information systems are used increasingly in all areas, offensive cyber operations have become involved in economic and industrial espionage. Countries and cybercriminal groups use complex techniques to enter company networks, stealing sensitive information, trade secrets, and intellectual property. The recognized APT29 group (a Russian hacker group), frequently associated with Russian intelligence services, is an example of a state-sponsored actor engaged in cyber espionage focusing on gaining sensitive information from various sectors. (Antoniuk, 2023)

Moreover, the role of offensive cyber operations extends to hybrid warfare, where cyber-attacks are combined with conventional military actions. Russian actors orchestrated the 2007 cyber-attacks against Estonia and the 2008 attacks against Georgia. Both were the first examples of combining cyber operations in a geopolitical

conflict (Lewis, 2015, pp. 4-7). Moreover, in Georgia, these activities were combined for the first time with traditional military actions.

From a manual perspective, the United States of America (USA) Army Field Manual (Cyberspace Operations and Electromagnetic Warfare FM 3-12) further categorizes offensive cyber operations into two types of actions:

1. Cyberspace Attack.
2. Cyberspace Exploitation.

While a cyberspace attack involves planned actions to achieve specific effects, cyberspace exploitation focuses on collecting information and enabling actions for future military operations (FM 3-12, 2021 pp. 2-7). In other words, to conduct offensive cyber operations, you must start with an exploitation action in a planned location to understand the vulnerabilities. As soon as the prerequisite requirements are in place and approved, it is possible to launch a cyber-attack to achieve the planned effects.

The named actions are achieved by the Common Tactical Mission Tasks like manipulate, suppress, destroy, etc. (FM 3-12, 2021 pp. 2-3) If we are going to look at this topic more widely, considering the different capabilities across different countries and drawing examples from publicly available sources we can see that offensive cyber operations can be a spectrum from sensitive to destructive actions. These actions may involve activities like deactivating computer accounts or even the whole domain or modifying passwords, slightly or destructively changing databases, ruining web pages, encrypting or deleting data, and potentially launching attacks that impact crucial infrastructure, such as electricity networks (Uren, et al., 2018 p. 6).

Offensive cyber operations can be used as a pre-emptive action to neutralize potential threats before they occur proactively. One of the good examples of this tactic was in Iran, where, most probably, Israel, in close cooperation with the USA, used the zero-day vulnerability to move the Stuxnet worm into the closed network. It is believed that the goal of this operation was to stop or delay the Iran nuclear program, which was also accomplished (Baezner et al., 2017, p. 4). Another positive aspect of cyber is having a military advantage against an opponent. It means that offensive cyber capabilities can complement traditional military operations, providing an additional advantage over adversaries without employing physical forces (Uren, et al., 2018).

As offensive cyber operations continue to develop, their scope involves a range of strategic military goals, including disrupting critical infrastructure, weakening political stability, and gaining technological authority over adversaries. These examples focus on offensive cyber operations of different and complex nature, highlighting their significance beyond traditional military functions. However, the comprehensive nature of offensive cyber operations requires careful consideration of legal, ethical, and diplomatic implications to guarantee responsible use, especially for Western countries.

1.2 Where can offensive cyber operations be used, and what are the possible effects?

In one of his articles, Tom Uren wrote that ‘offensive cyber operations are distinct from cyber-enabled espionage, in which the goal is to gather information without having an effect.’ (Uren, et al., 2018) In this section, I will explore where it is possible to use complex offensive cyber operations. I will discover their utilization within the intelligence community and defense forces. Investigating specific instances, legislative influences, and the relationship between cyber forces and intelligence services. All this provides valuable awareness of the changing dynamics of cyber warfare. Furthermore, in this paragraph, I will discuss the possible effects of offensive cyber operations, considering their role as shaping enablers and the complex balance between intelligence gathering and the activation of cyber capabilities.

Cyber has been a significant resource for intelligence services for decades, and the intel community wants to keep this asset under its control. However, with the latest developments, this means moves for multiple owners, it is a turning point for defense forces, and offensive cyber operations are forcing intelligence-focused silos to share the medium (Laudrain, 2019). In Norway, this is also the factor that causes offensive cyber operations capabilities to be placed under the jurisdiction of intelligence services (Liebertrau, 2022 pp. 138-139). Why? This is purely because the cyber domain is a significant resource for intel, the level of coordination is more manageable, and it is more cost-effective. Moreover, it is also related to legislation in specific countries. In Norway, the law obligates the armed forces to conduct only cyber defense operations. However, the offensive operations are planned and conducted by Intelligence services. (Liebertrau, 2022 pp. 138-140) Through espionage campaigns where cyber is a

platform, it is possible to achieve planned outcomes (Muller et al., 2023, p. 16). Consequences or effects from espionage can be classified information, trade- or other industrial secrets that can be used as an advantage.

Most of the time, vulnerabilities in some networks are the so-called 'door into the system' for intel gathering. At the same time, this is an entry point for cyber forces to put some malware into the system. Moreover, now comes the conflict. If the cyber community wants to deliver some effects they must activate the malware, at the same time, most probably, intel services are losing this resource because the system is not usable anymore, or the vulnerability will be fixed (Jacobsen, 2021 p. 712).

Offensive cyber operations play a significant role in modern military strategies, integrating cyber capabilities into combined arms or joint warfare has become increasingly dominant. Why? This way, it is possible to create multiple dilemmas for an adversary (Muller, et al., 2023 lk 5). If a particular service is ineffective, shifting the focus to shaping efforts is possible, and another component can accomplish decisive actions. Another option to achieve a comprehensive strategic advantage with offensive cyber capabilities is to use these elements as force-multiplier capabilities (Smeets, 2018 p. 105). Some scholars also say that cyber will be more likely to be used as a shaping enabler in the future to influence strategic communication (Muller, et al., 2023 p. 16). Propaganda or information campaigns use cyber as a platform to target audiences. The effect of well-planned and executed propaganda or information operations can be devastating. If effective, it can cause chaos and political instability in society (Muller, et al., 2023). This is already an effect that helps achieve strategic goals.

Offensive cyber operations are designed to disrupt, disable, or exploit adversary IT systems. Military forces aim to achieve strategic advantages by employing offensive cyber tools while minimizing the need for direct physical engagement. Jacobsen brings out that cyber capabilities must be redundant for conventional forces, which means that capability is an asset if the target is unavailable for kinetic forces (Jacobsen, 2021 p. 720). One good example of the military's use of offensive cyber operations is the Stuxnet virus, which came to the public in 2010. Stuxnet was an advanced cyber weapon, and it is believed that 'the worm' was developed jointly by the United States and Israel. It was explicitly designed to target Iran's nuclear facilities to disrupt its

uranium enrichment capabilities. By penetrating computer systems and manipulating industrial processes, Stuxnet demonstrated the potential of offensive cyber operations to sabotage critical infrastructure in a targeted and hidden manner. (Baezner, et al., 2017 pp. 4-6)

In the last decade, integrating offensive cyber operations into military doctrines has become more crucial. Nations have established dedicated cyber commands responsible for developing and deploying cyber capabilities to enhance military capabilities. Muller brings out that in the future, great powers will continue to invest in cyber outside of intelligence and deception capabilities. However, the return will decrease, and cyber will play a supportive and shaping role in the major conflicts (Muller, et al., 2023 p. 1). In most cases, offensive cyber operations do not cause the same effect as kinetic attacks but can disrupt, deny, or even damage specific hardware, software, and online services. The effect of not having access to damaged services is degreasing morale, which is like strategic bombing but without mass destruction (Lewis, 2015 pp. 3-5).

The United States of America (USA) Army Field Manual (Cyberspace Operations and Electromagnetic Warfare FM 3-12) says that cyber operations are divided into three types of operations:

1. Department of Defense Information Network Operations.
2. Defensive Cyberspace Operations (DCO).
 - a. DCO Internal Defense Measures (DCO-IDM).
 - b. DCO Response Actions (DCO-RA).
3. Offensive Cyberspace Operations (OCO).

Under the named Cyberspace Operations, they conduct four types of cyberspace actions.

1. Cyberspace Security.
2. Cyberspace Defense.
3. Cyberspace Attack.
4. Cyberspace Exploitation.

Actions are achieved by the Common Tactical Mission Tasks like secure, clear, neutralize, etc. There are only six effects that the US armed forces are planning to reach via cyber operations:

1. Degrade.
2. Deny.
3. Disrupt.
4. Destroy.
5. Deceive.
6. Suppress.

Out of six effects, only one is named differently from the effects that land forces reach throughout land operations. (FM 3-12, 2021 pp. 2-7) In cyber, the effect of deceive is achieved when someone tricks another person into believing something false. This is successful when the deceived person believes something untrue, and the one who initiated the effect usually benefits from this situation. (Grant pp. 218-220)

Cyber is a strategic domain that enables several activities. Offensive cyber operations can be used for different functions and have various effects. Offensive cyber operations serve the fruitful interest of cyber espionage, where the intent is to stealthily gather intelligence information, typically without the target's knowledge. However, states increasingly understand the essence of offensive cyber operations, which involve a broader range of malicious activities aimed to cause denial or disruption of services, including communication channels to support kinetic actions. The effect of named capabilities can significantly hinder the adversary's ability to mobilize and sustain military operations and destabilize the local society. However, both cyber espionage and offensive cyber operations are significant fears in the scope of cybersecurity. Organizations and governments must implement robust security measures to defend against these threats. Additionally, distinguishing between the two is crucial for appropriate threat analysis, response, and attribution.

1.3 What are the risks and challenges of using offensive cyber operations?

In an era where digital connectivity supports nearly every aspect of modern society, the utilization of offensive cyber operations has appeared as an effective tool for state and non-state actors what they are willing to use. However, alongside the potential benefits, these actions always have challenges and risks. Dilemmas will come exceptionally quickly when we bring NATO into this *modus operandum*. In this paragraph, I will investigate the principal risks and challenges if offensive cyber capabilities are used.

In February 2022, Russian enthusiasts organized a cyberattack against Viasat. This is a good example that shows possible unknown risks and dimensions of offensive cyber activity. Initially, the target was the Ukrainian Command and Control (C2) system, which relied on a civilian-owned transmission channel. The result of this operation was that the Ukrainian C2 channel was not useable. However, the implications were visible in the German energy sector, with nearly 6,000 wind turbines requiring manual updates because the remote monitoring access was lost (O'Neill, 2022). Also, thousands of home users were affected across different European countries (Gatlan, 2022). We do not know if the risk was acceptable for the organization that launched the attack or if it was an unplanned consequence. However, it is a perfect case to highlight the cyber complexity between stakeholders and the planned effect versus the actual effect. Jacobsen brings another risk related to offensive cyber activities under the NATO umbrella. He sees the possibility of unintended conflict escalation, which means that cyber activities are declared by an adversary as military preparations (Jacobsen, 2021 p. 719). From a Strategic Communication perspective, it is a problem because, from the *modus operandum* point of view, NATO is a collective defense organization. On the other hand, it has been stated clearly that cyber-attacks against the state could prompt a collective response under Article 5 (Pruckova, 2023). This is a clear statement from the defense organization for possible opponents that cyber-attacks against NATO are not any more risk-free.

Moreover, sometimes cyber espionage could be taken as a cyber-attack by the adversary, mainly when activities are carried out against nuclear facilities, and this way, there is a considerable risk of escalation (Acton, 2020 p. 133). Offensive cyber activities are focused on vulnerabilities in adversary ICT systems. However, in the context of NATO, if one country offers to deliver cyber effects in support of some NATO operations, it might close the intel resources for another country because both use the same vulnerability to enter into adversary systems (Jacobsen, 2021 p. 713). Moreover, in NATO, offensive cyber activities create dilemmas between goals and tasks because of the use of the cyber domain. The question remains: Do we need to collect intel information or launch cyber operations? The problem behind this dilemma is that decisions to collect intelligence are made nationally. However, offensive cyber operation activation is done on the NATO military command structure or a national level. (Lewis, 2015 p. 9) Another topic is situational awareness. It is a standard

common understanding in military units that reports and returns include unit locations and assessing how effective troops are in fulfilling tasks. All this supports situational awareness between units. On the physical battlefield, it is easy to count tanks and other means of equipment. Counting all the cyber capabilities on the virtual battlefield is complex, meaning the assessment must be done objectively (Schulze, 2019 p. 5). Why? It is related to situational awareness and willingness to share information. If units do not share the situation with neighboring units, it is easy to target each other, and the whole activity is ineffective.

Another negative fact associated with offensive cyber operations is the unintended consequences, causing harm to third parties, critical infrastructure, or systems essential for public services like the Viasat case in Ukraine. Moreover, cyberspace infrastructure is globally interconnected and human-made, usable for anyone for very different purposes. This also means that offensive cyber operations can have global consequences that affect the involved parties and disrupt the international community. All this can burden diplomatic relations and lead to broader geopolitical concerns. (Lewis, 2015)

The combined arms approach has been the way in the last decades how the Western community has been preparing and fighting in the last conflicts. Combined arms warfare is complex due to the high coordination and synchronization requirements. The combined effects in the cyber domain are particularly challenging due to the tendency for non-smooth outcomes, persistent uncertainty, and natural tension associated with using force (Muller, et al., 2023 p. 16).

Looking at the risks and challenges associated with offensive cyber operations, we see that modern cyber warfare is complex. We must balance offensive actions with strengthening our cyber defenses and understand that working with other countries is vital. It is essential to highlight the dimensions of unintended consequences because cyber is the global domain. As countries deal with these challenges, focusing on improving cyber defenses and working together internationally to handle more significant issues is crucial. Overall, this shows us how complicated cyber warfare is and why we must be flexible and work together to deal with it effectively.

1.4 What are the effects of offensive cyber operations on national security?

In the complicated landscape of contemporary warfare, combining cyber capabilities with traditional military strategies has become a foundation of national security discussion. In this paragraph, I will find the answers to the question of the effects of offensive cyber operations on national security.

Smeets defines offensive cyber capability as entering computer systems or networks to affect or damage possible information and hardware (Smeets, 2018 p. 6). In both conventional military operations and cybersecurity, it is the well-known principle that maintaining a continuous and robust defensive posture is essential. However, offensive operations are best conducted with careful preparation and training, activation of offense should be accurate and resultant (Muller, 2019 p. 1). From this point, we can conclude that if the offensive activity with conventional forces is effectively implemented, the forces are probably viable and reusable to provide security. However, in the cyber domain, one specifically prepared mission is usable only once. As soon as the offensive cyber activity is launched, you can be sure that this vulnerability or access point will be fixed. During the Second World War, Germans pioneered integrating land-, air- and navy services. Jacobsen is adding to this concept cyber as well. He says that the expectations for cyber effects are high nowadays, especially when discussing the operational context. It is necessary to integrate cyber capabilities with other means that are more tangible to achieve operational effects (Jacobsen, 2021 p. 708). It means that when we are talking about cyber on combined arms or joint operational level, cyber is often an independent service that usually shapes effects for an operation or neighbor services (Muller, et al., 2023 p. 2). Muller also emphasizes the importance of integrating offensive cyber operations with other effects like information operations to create multiple dilemmas for an adversary (Muller, et al., 2023 pp. 5-10).

In the 21st century, information stands as a precious resource. The expectation is that information moves relatively quickly between state agencies and society, which is one of the backbones of state security. The information flows require a medium, nowadays, the majority of the information is digital (Hilbert, et al., 2011). Cyberspace is essential for digital information. In Allied Joint Publication (AJP-3.20) cyberspace is defined as a three-layer environment: physical-, logical- and cyber persona layer (AJP-3.20, 2020 p. 3). Establishing effective transmission channels (physical layer) is essential to enable the dissemination of digital information. Transmission channels are constantly

expanding, owned by private companies and national governments (Laudon, et al., 2007) (Muller, et al., 2023 p. 3). That is also why states and the military depend on civil networked technologies (Jacobsen, 2021 p. 720).

In the scope of information operations, cyber functions as a significant enabler. This facilitation predominantly occurs within the cyber persona layer in the digital landscape. When targeting a diverse range of governmental and non-governmental services, such as emergency services, logistic facilities, military command and control centers, online banking, and online news channels, and simultaneously launching an information operation with tailored narratives, it becomes feasible to rouse societal chaos. This state of the abyss can influence and disrupt the adversary's decision-making processes and organizational structures. Simultaneously, it serves to protect one's society. (Muller, et al., 2023 pp. 2-5) Information operations in the cyber domain are now commonplace (Adbyraev, 2020). Weaknesses in cyber defense within various organizations make society vulnerable, posing a relatively high risk to national security. The facts mentioned above are also the main reasons why cyber defense is an essential element for state security at the military and state levels. Information and services must be available for society constantly, which is one of the primary roles of the state. If interruptions occur constantly in service delivery, information is not available, or it is permanently manipulated, there is a high risk to state security. That is one of the reasons why stability in services is essential for service providers and states. Cyber as an environment is increasingly important for states and societies because it enables them to save resources like time and money. More importantly, it is a vital channel for exchanging information as data moves in the cyber domain at the speed of light. It is becoming increasingly clear that cybersecurity has become synonymous with national security in the era of blurred lines regarding cyber-attacks (Striem-Amit, 2021).

Another option is to amplify or shape kinetic military actions via the cyber domain. This happens mainly on the logical layer. One of the first real-world examples is the Viasat cyberattack, where Russian hackers disrupted and destroyed private company communication capabilities used by the Ukrainian military (O'Neill, 2022). This is an excellent example of using cyber in joint military operations to shape the environment for neighbor services. However, it also illustrates the importance of cyberspace security and its possible implications for national security.

The intelligence community, a crucial element of national security, utilizes offensive cyber operations to collect information about potential threats to national security. This is achieved by infiltrating adversary networks or gathering information from open sources. We get information about the potential adversaries intentions, capabilities, and actions from different sources. With sufficient information, taking pre-emptive actions to mitigate or neutralize possible threats is possible. Therefore, offensive cyber operations can be a pre-emptive approach to prevent potential threats. A good example is the Stuxnet case, in which the USA and Israel used offensive cyber operations to sabotage hostile plans before they could be executed. This way, it is possible to mitigate risks to national security without using kinetic force elements.

Offensive cyber operations can have an extreme and beneficial impact on national security, offering opportunities to disrupt adversaries, gather intelligence, and maintain strategic advantage. However, they also involve risks, including escalation, vulnerability exposure, and legal or ethical concerns, which must be carefully analyzed and managed to safeguard national interests effectively.

Conclusion

This research has explored the complex field of offensive cyber operations and their implications for national security in the current period. Through a comprehensive analysis of various factors, it is clear that offensive cyber capabilities have emerged as critical tools in modern military strategies, reshaping the dynamics of warfare and state defense mechanisms. It is essential for nations to build up offensive cyber capabilities and to speak about these more openly because offensive activities are an essential part of cyber defense and state security. Also, it is critical to speak about offensive cyber operations in the joint force context, only in this way is it possible to amplify the effects of joint influence between services and to provide deterrence, which is essential for national security (Van de Velde, 2023). In the future, offensive cyber operations will likely play more and more supportive or shaping rather than decisive roles in major operations on the battlefield (Muller, et al., 2023 p. 1). Offensive cyber operations are complex and unpredictable, with strategic advantages and potential risks. To use named capabilities responsibly and reasonably, planning carefully and in detail and thinking about the operations legal, ethical, and diplomatic implications is essential.

Cyber is playing a vital role already now. The physical and logical layers bring together battle networks, intelligence support, and information exchange in a way that gives the persona layer comprehensive access to information and allows decision-makers to make decisions based on adequate information. Offensive cyber operations are not absolute weapons, meaning these capabilities usually do not fulfill decisive actions but are beneficial. That is also why traditional armed forces are still required for states.

Cyber is not a national domain, it facilitates capabilities to conduct kinetic and non-kinetic operations. Since we do not have borders in the cyber domain, achieving effects abroad without crossing physical borders is possible. In the cyber domain, permanent cooperation and coordination between stakeholders are vital activities that can positively affect state security. Cyber is an essential domain for state and society because society and private companies are the primary consumers of these services that are provided via cyber. Moreover, in Western countries, where most of the services are provided by private companies, it is essential to understand that these private companies also have a significant role in providing public services in the state, and this way, they support security in the state. One of the key takeaways from this research is the changing nature of offensive cyber operations, which have expanded beyond traditional military objectives to cover a wide range of strategic goals. From manipulating public opinion to economic espionage and hybrid warfare, offensive cyber activities have become fundamental to shaping state interests and utilizing power in the human-made domain.

As the warfare landscape develops, offensive cyber operations remain a dynamic and essential component of military strategy and state security. Offensive cyber operations present both opportunities and challenges for national security. While they offer strategic advantages such as pre-emptive neutralization of threats, intelligence gathering, and force multiplication, they also entail risks such as unintended consequences, escalation, and vulnerability exposure. The challenge sits in balancing the interest of strategic advantages with the ethical considerations and potential consequences associated with using these capabilities in conflicts to support state interest.

To get a shaping effect from offensive cyber operations for state security it is important to focus on the following ideas. It is essential to invest in offensive cyber capabilities.

Investment should include hardware, software, and technicians. Starting as soon as possible is essential because the mutation process from elements into capabilities only occurs slowly. Interagency coordination and cooperation must be forced, only this way is it possible to achieve positive effects in the cyber domain. Additionally, states must promote the public sector to enhance cybersecurity, critical infrastructure, and services. Triangles (governmental agencies, private companies, and universities) are the main stakeholders that control resources and expertise to address and solve cyber threats more efficiently. If the state is developing offensive capabilities, we cannot exclude investments in cyber resilience. This includes enhanced cybersecurity, proper incident management, and capabilities to detect and mitigate cyber threats effectively. Finally, all institutions need to be adaptable and flexible when speaking about cyber. Only in this way is it possible to solve cyber challenges effectively in an increasingly digitized world and uphold the principles of a ruled-based world order.

Bibliography

Acton, James M. 2020. Cyber Warfare & Inadvertent Escalation. *Meeting the Challenges of a New Nuclear*. s.l. : Daedalus , Spring 2020, 2020. Vols. Vol. 149, No. 2.

Adbyraev, Cholpon. 2020. The Use of Cyberspace in the Context of Hybrid Warfare. s.l. : Austrian Institute for International Affairs, 2020.

AJP-3.20. 2020. Allied Joint Publication for Cyberspace Operations. s.l. : NATO Standardization Office, 2020. Vol. Edition A Version 1.

Antoniuk, Daruna. 2023. Cyber-espionage operation on embassies linked to Russia's Cozy Bear hackers. 2023.

Austin, Greg, Tay, Kai Lin and Sharma, Munish. 2022. Great-Power Offensive Cyber Campaigns: Experiments in Strategy. 2022.

Baezner, Marie and Robin, Patrice. 2017. *Hotspot Analysis: Stuxnet*. Zürich : Center for Security Studies (CSS), ETH Zürich, 2017.

Clausewitz, Carl Von. 1946. *On War*. 1946.

FM 3-12. 2021. Cyberspace Operations and Electromagnetic Warfare. s.l. : USA Department of the Army, 2021.

Gatlan, Sergiu. 2022. Viasat shares details on the KA-SAT satellite service cyberattack. [Online] 30 March 2022. [Cited: 16 October 2023.]

<https://www.bleepingcomputer.com/news/security/viasat-shares-details-on-ka-sat-satellite-service-cyberattack/>.

Grant, Tim. Detect, Deny, Degrade, Disrupt, Destroy, Deceive: Which is the Greatest in OCO?

Hilbert, M and Lopez, P. 2011. The world's technological capacity to store, communicate, and compute information. *Science Express*. 2011.

Iasiello, Emilio. 2014. Is Cyber Deterrence an Illusory Course of Action? *Journal of Strategic Security*. 2014. Vol. Volume 7, Article 6.

Jacobsen, Jeppe T. 2021. Cyber offense in NATO: challenges and opportunities. *International Affairs* 97:3. s.l. : Published by Oxford University Press on behalf of The Royal Institute of International Affairs, 2021.

Laudon, Kenneth C and Laudon, Jane P. 2007. Management Information Systems. [Online] 2007. [Cited: 6 October 2023.] <https://paginas.fe.up.pt/~als/mis10e/ch7/chpt7-3bullettext.htm>.

Laudrain, Arthur P.B. 2019. France's New Offensive Cyber Doctrine. *Foreign Relations and International Law*. 2019.

Lewis, A James. 2015. The Role of Offensive Cyber Operations in NATO's Collective Defence. *A NATO CCDCOE Publication on Strategic Cyber Security Tallinn Paper*. Tallinn : s.n., 2015. Vol. No. 8.

Liebertrau, Tobias. 2022. Organizing cyber capability across military and intelligence entities: collaboration, separation, or centralization. 2022.

McKinsey and Company. 2023. <https://www.mckinsey.com>. <https://www.mckinsey.com>. [Online] 14 June 2023. [Cited: 04 03 2024.] <https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-digital-transformation>.

Muller, Grace B, et al. 2023. Cyber Operations during the Russo-Ukrainian War. 2023.

Muller, Lilly Pijnenburg. 2019. Military Offensive Cyber-Capabilities: Small-State Perspectives. *Norwegian Institute of International Affairs*. 2019. Vol. 1/2019.

O'Neill, Patrick Nowell. 2022. Russia hacked an American satellite company one hour before the Ukraine invasion. [Online] 10 May 2022. [Cited: 15 October 2023.]

Pruckova, Michaela. 2023. Cyber attacks and Article 5 - a note on a blurry but consistent position of NATO. s.l. : NATO CCDCOE, 3 August 2023.

Schulze, Matthias. 2019. Cyber deterrence is overrated: analysis of the deterrent potential of the new cyber doctrine and lessons for Germany's "active cyber defense". Berlin : Deutsches Institut für Internationale Politik und Sicherheit, 2019. Vol. 34.

Smeets, Max. 2018. A matter of time: On the transitory nature of cyberweapons. Oxford: The Journal of Strategic Studies, 2018. Vol. Vol. 41.

—. 2018. The Strategic Promise of Offensive Cyber Operations. 2018, Vol. Vol 12 No 3.

Striem-Amit, Yonatan. 2021. Cybersecurity is National Security. [Online] 2 September 2021. [Cited: 1 November 2023.] <https://www.cybereason.com/blog/cybersecurity-is-national-security>.

Uren, Tom and Hanson, Fergus. 2018. Australia's offensive cyber capability. 2018.

Van de Velde, James. 2023. Cyber Deterrence Is Dead! Long Live “Integrated Deterrence!”. s.l. : Joint Force Quarterly, 2023. Vol. 109.

LAURYNAS SINICA. Application of doctrinal special operations warfare during the war in Ukraine and its adaptation to contemporary military conflicts.

Introduction.

‘Immortals... We will put their name to the test.’

King Leonidas of Sparta, amidst the battle of Thermopylae.

Despite being a product of comprehensive historical practices, there is no better test for a warfare doctrine than an actual battle engagement. Assessment or exercise in a simulated or virtual environment could hardly match this test. Although undesirably, the current war in Ukraine represents a unique opportunity to evaluate whether established documents, methods, and concepts of warfare are still prone, valid, and appropriate for a similar type of state-to-state conflict in the modern era of technological, cyber, and space developments (Jones et al., 2023). During recent years, especially after the closing down of Operation Enduring Freedom and Resolute Support Missions in the Islamic Republic of Afghanistan in 2021, many world leaders, scholars, and practitioners discussed the purpose, way ahead, and application of the NATO Alliance itself, state military as an instrument of national power and influence, and the overall future requirements throughout the full spectrum of domains and branches of service.

Tangible steps were taken. At the 2022 Madrid Summit, NATO leaders took decisions that set the Alliance's direction for the near and long-term future. They approved a significant reconditioning of collective defence and deterrence, updated defence plans with more forces at high readiness and designated forces to defend allocated territories of the Alliance (NATO, 2022). At the 2023 Vilnius Summit, NATO leaders modernised the Alliance for a new era of collective defence. To respond to a radically changed security environment, they asserted to strengthen NATO's collective defence against all threats from all directions. States would individually and collectively deliver a complete range of capabilities, forces, resources, plans, and infrastructure needed for deterrence and defence, including high-intensity, multi-domain warfighting against nuclear-armed peer competitors (NATO, 2023).

The abovementioned strategic decisions avalanched a dilemma for all military branches in reevaluating and reconsidering their status in the new reality. This research aims to identify how the main Special Operations Forces (SOF) tasks, seen through the lens of NATO Allied Joint Publication – 3.5 (AJP-3.5) Allied Joint Doctrine for Special Operations – direct action, special reconnaissance, and military assistance, fit in the battlefield during the contemporary war in Ukraine. This paper will argue that after a harsh examination of the war in Ukraine, SOF doctrinal core tasks remain the essence of the special operations (SO) warfare but should be reviewed and updated regarding SOF's role, types of operations, and required equipment in a state-on-state military conflict environment.

The first chapter will introduce the nature of SO warfare and doctrinal SOF tasks as per NATO AJP-3.5. Chapter 2 will deliver an overview of the Ukrainian SOF and case studies of their operations throughout the full spectrum of core SOF missions. It will enable an assessment of the doctrinal approach to SO warfare and an evaluation of its relativity on the present-day battlefield. Analysis methods will also include a review of available literature and research of descriptive, mostly secondary data sources due to sound reasons – the sensitive and classified nature of SOF operations and limited direct access to eyewitnesses and direct participants. Finally, the conclusions and recommendations portion will provide overall findings and suggest possible NATO SOF doctrine adjustments to efficiently deliver options for operational and strategic commands in the new era of warfare. The research aims to grasp the gained experience from this illicit and unfortunate full-scale war and suggest possible ways to incorporate it into the Western domain's SO warfare.

Chapter 1. Special operations warfare – doctrinal SOF definitions and tasks.

SOF and their functions in recorded warfare history have not changed much. At all times, military commanders have grasped the advantage of specially selected and purportedly trained groups of operators that could provide offensive spirit to the campaign and desired effects not only by eliminating or destroying nominated targets, but also by delivering reconnaissance missions, military liaison, force multiplication, and other valuable outcomes. Especially in cases where the deployment of large-scale regular military formations could not deliver (Sof, 2012). Titulaer (2021) states that the lasting strategic value of SO comes from its ability to partly fill the empty military force space left unfulfilled by regular units due to organisational limits. Doctrinal military

solutions cannot always offer viable answers to all problem sets, especially when challenged by out-of-ordinary circumstances (Watling, 2021). Scholars and practitioners suggest retaining a certain level of ambiguity and not binding SO to firm formulas or definitions because they are often unique in some element, equipment, or environment (Solli, 2021).

Despite being in a military alliance, a few big nations, especially the United States of America (USA), describe and formulate SO slightly differently (JSOU, 2023), with a tendency to have more comprehensive options for action (Solli, 2021). USA Department of Defence Joint Publication 3-05 Joint Doctrine for Special Operations (2020) divide SO into 12 core activities. Regardless, at the operational and strategic levels, focusing on the effects of SO rather than their tactical nature would be more constructive.

There is also a discussion that these norms led to unnecessary competition between military branches to increase the autonomy of their organisations and the stake of limited resources. Colonel (retired) Hooker Jr. (2023) argues that inexistent command relationships, lack of accountability to Joint Force commanders, poor coordination, deficiencies in combined training, absence of interoperability, and different organisational approaches to regulations and standards lead to conflict and cause distrust between SOF and conventional communities, while also questioning SOF strategic level deliverables. On the other hand, there exists an argument that conceivably more significant is the required change of position among strategic and operational commanders to untether SOF units, stating that the existing requirement for real-time information diminishes their ability to operate in high-risk environments. Allowing SOF to train, experiment, and, sometimes, flunk is essential in finding the best ways to accomplish the tasks (Watling, 2021). It seems that this discourse arises from a different point of view – a conventional side of the military trying to accomplish a tactical level mission by all means and SOF scholars seeking ways to instrumentalise SOF in providing necessary tools to solve non-typical problem sets. Without a profound understanding of SO, it is quite a common fallacy to assign SOF units to support conventional ones, which do not possess the ability to provide the required level of precise intelligence data, combat support (CS), specially adapted combat service support (CSS) and such (Solli, 2021).

There are limitations to the use of SOF, as it should be primarily employed only in critical or decisive operations, and, most importantly, SOF should not be used as an alternative to conventional forces (NATO, 2019). As per the widely acknowledged Five SOF Truths – competent and well-prepared SOF cannot be rapidly created nor easily replaced due to a devotion to quality instead of quantity and aspiration towards suitable individuals rather than hardware (Collins, 1987). Moreover, due to logistical, capacity, and general survivability restraints, SOF often greatly relies upon support from other Armed Forces components or other state institutions (Watling, 2021). This reveals that inadequate use of SOF can speedily lead to the depletion of its capabilities.

Nevertheless, as this research aims to examine the application of doctrinal special operations warfare during the war in Ukraine, a basis for common understanding is required to establish shared comprehension and interoperability in the planning and execution of SO. AJP-3.5 is a NATO-established standard where SO are described as a military activity conducted by specially selected, organised, trained, and equipped personnel using distinct organisational culture, methods, and modes of engagement (NATO, 2019). Usually, SO are conducted across the full spectrum of conventional military operations. However, the main difference is in acceptance of a certain degree of political or military risk for achieving strategic or operational effects (Titulaer, 2021). SOF principal tasks comprise direct action (DA), special reconnaissance (SR) and military assistance (MA), which could be included in a required combination altogether or separately (NATO, 2019). Doctrinally, the proportionality of demand in those three distinct mission sets varies throughout the spectrum of conflict – from a prominent MA role in peacetime to a significant DA segment during armed conflict (NATO, 2019). The following paragraphs will describe the core SOF tasks defined in AJP-3.5.

1.1. Direct action.

DA operations are the SO mission set's most prominent and visible portion. They sometimes induce the prejudice that SOF 'just want to kill them all' (Solli, 2021). It is often understood as a vicious kinetic military action to destroy designated targets of operational or strategic value, distinguished by the level of accurate intelligence, strike precision and utilised tactics, techniques, and procedures. In AJP-3.5, DA is described as 'a short-duration strike or other small-scale offensive action to seize, destroy, capture, recover, or inflict damage to achieve specific, well-defined and often time-

sensitive results'. DA can include raids, ambushes, and assaults, terminal guidance operations, recovery operations and precision destruction operations (NATO, 2019).

As with the rest of SO, DA differs from conventional offensive operations in the level of risk, methods and capabilities employed, and the degree of very high precision on specific, well-defined, and developed targets. DA operations create a specific strategic or operational effect, usually including a projected withdrawal from the target area (NATO, 2019). DA operations are not meant to seize, especially not to hold terrain. Also, DA could be conducted independently, supported by or in support of conventional forces. An essential element of DA is that it must be asymmetric, with the goal being to pressure the enemy to give out more limited resources to prevent an attack than expenditures to carry it out (Watling, 2021). Asymmetric also means that the action plan needs to cover an achievement of relative superiority for a required timeframe to inflict desired results on the target (McRaven, 1996).

1.2. Special reconnaissance.

SOF intelligence collection can provide at least a couple of deliverables: developing actionable intelligence for follow-on kinetic actions or situational awareness and assessing a specified target or area before, during and after an operation by placing persistent or non-persistent eyes on the target (Westberg, 2016). As part of the intelligence collection process, SR, by utilising various intelligence disciplines and methods, could potentially create a relative certainty where constraints are imposed by acceptable risk levels, hostile countermeasures, other systems' availability, weather, terrain, and similar restrictions (Solli, 2021).

AJP-3.5 defines SR as:

Reconnaissance and surveillance activities conducted as a special operation in, but not limited to, hostile, denied, or diplomatically and/or politically sensitive environments to collect or verify information of strategic or operational significance, led by SOF using distinct capabilities, techniques and modes of employment.

SR can include environmental reconnaissance, threat assessment, target assessment, and post-action reconnaissance. SOF may conduct these tasks separately, supported by, in conjunction with, or in support of other components (NATO, 2019).

Despite vast technological advances in intelligence, surveillance and reconnaissance (ISR) platforms, the importance of the human aspect on the battleground remains valid, not only for entities that do not have advanced technology, but also when there is an absence or lack of required collection platforms in the theatre of operations due to various reasons of physical distance, risk, or other limitations (Westberg, 2016).

1.3. Military assistance.

MA is the broadest category of SOF core activities, where various types of support measures are provided to a wide range of recipients ranging from military tactical units to non-military actors such as local, regional, or national leadership, ministries, or organisations (Solli, 2021). SOF could provide training, advising, mentoring, partnering, or conduct operations to support, enable, and influence critical friendly assets. According to AJP-3.5, MA activities include training, advising, mentoring, partnering, and interagency support (NATO, 2019). SOF becomes especially useful in cases where national interests should be hidden under the shade and regular military force deployments are not feasible.

The extensive use of MA during peacetime comes from a tendency of large countries, especially the USA, to use a combination of MA activities for interinstitutional and inter-military network building to forge relationships and alliances well ahead of crises. There is a widely recognised need to start those as early as possible, and a very limited number of organisations within the military instrument of national power have as much experience in working with allies and partners as SOF (Taft et al., 2019).

Doctrinal MA activities are primarily described as conducted abroad, where indigenous cultural and governmental nuances can substantially alter operations. This approach is a legacy of long-lasting international security force assistance, stabilisation, and reconstruction missions in the Middle East (Watling, 2021). Doctrine does not reference internal national elements, requiring assistance to increase resilience and armed or unarmed resistance. That often raises dilemmas for smaller states on the possibility of employing national SOF for internal MA activities to support national military or paramilitary organisations as described in Resistance Operating Concept, released by USA Special Operations Command Europe (2019).

Chapter 2. Ukrainian SOF and their operations during the Russo-Ukrainian War.

Current Ukrainian Special Operations Forces (UASOF), having a long-lasting legacy of a Soviet-era type of *Spetsnaz* units, were established, dismantled, and re-established several times in response to the various crises that emerged throughout history (Dieanu, 2022). Finally, in 2015-2016, UASOF was set on track legally and resourcefully to develop as a Western-style SOF organisation as a separate branch of service of the Armed Forces of Ukraine (Momi, 2022). Verkhovna Rada (2016), in the national legislation of Ukraine, defined SO as:

A set of coordinated and interrelated in purpose, tasks, place and time of special actions of units of the Special Operations Forces of the Armed Forces of Ukraine, aimed at creating conditions for achieving strategic (operational) goals, which are carried out according to a single plan independently or in cooperation with military units, other units of the Armed Forces of Ukraine, other military formations, law enforcement agencies of Ukraine and other components of the defence forces.

Currently, UASOF has eight tasks, which are (1) Measures of the legal regime of martial law and state of emergency; (2) Military information and psychological operations; (3) Protection of life of citizens and objects of state property outside Ukraine; (4) Participation in the fight against illicit trafficking of weapons and drugs; (5) Organisation and support of resistance movement; (6) Combating terrorism and piracy; (7) Maritime Safety of Ukraine; (8) International military cooperation (UASOF, 2016). To fulfil these tasks and to have the ability to provide the full spectrum of SO according to NATO standards, UASOF comprises various types of separate land and maritime units (White, 2022a). The notable distinction is a separate component for psychological operations (Wilk, 2017).

UASOF training and equipping were expedited by many NATO countries, including Canada, Denmark, Estonia, Latvia, Lithuania, Poland, Romania, the United Kingdom, the USA, and others (White, 2022a). Extensive and rigorous training was conducted in Ukraine and abroad (Borsari, 2022). UASOF participated in many international joint military exercises (Momi, 2022). One of the most significant achievements of UASOF – positive certification of a Special Operations Task Group for a stand-by as an element of the NATO Response Force (Sanders, 2023) – was attained during the annual international exercise Flaming Sword 2018 in Lithuania as an outcome of a long-lasting working partnership with Lithuanian SOF (Unian, 2019).

UASOF had only six years to prepare for the current total state-to-state war. During that short period, vast organisational, mindset and habitual shifts were implemented. Due to broad Western coalition support for the transformation process, UASOF swiftly adopted the main principles of SOF formation – voluntary basis, selection, and special preparation. With training at NATO standards, access to sophisticated equipment (night vision, ISR, encrypted communications), and experience from combat engagements in the Luhansk and Donbas regions, UASOF became a credible force, operationally prepared to oppose the Russian full-scale invasion on 24 February 2022. A case of every core SOF task application will be analysed in the following paragraphs.

2.1. Direct action: battle for Kyiv.

On the first days of the attack, Russians adhered to their military offensive doctrine – it started with a massive electronic warfare, missile, and air attack, followed by an airborne assault to seize critical objectives and create favourable conditions for follow-on forces (Borsuk, 2023). Successful execution would have enabled them to take over strategic legislative and infrastructure assets swiftly, replace the legitimate government, and impose control over the whole state (USDoA, 2024). One of the key objectives in their plan was the Hostomel airport in the vicinity of the capital, Kyiv. Airborne troops were supposed to secure the runway to receive cargo aeroplanes with armoured vehicles, heavy weapons, and second-echelon personnel (Stojar, 2023). The other key objective was the city of Irpin, where command and control (C2) nodes were to be established. Lastly, two main roads from Belarus were to be used as a main axis of advance towards Kyiv (Dieanu, 2022).

Russian paratroopers, who managed to land at Hostomel airport, quickly became an isolated target. A 60 km long massive Russian armour and logistics convoy from Belarus failed to break through. They endured tremendous losses from UASOF, territorial-guard units, unmanned aerial drones and artillery (Watling, 2022). According to available sources, UASOF had a significant role in repelling Russian forces from Hostomel airport and other approach directions (White, 2022b). UASOF units spurred the defence of strong points in urban terrain along the roads or infiltrated towards the northern part of Ukraine to attack Russian logistical convoys (Sanders, 2023). They conducted robust DA operations to cause significant damage to critical targets of the Russian military (Dieanu, 2022). Several pieces of evidence indicate that the UASOF operators performed remarkably well against a comparably larger and stronger

opponent. Borsari (2022) agrees that this derived from greater tactical skills and the ability to operate at night but also admits that poor adversary operational planning, tactics, deficiency of coordination and combined arms manoeuvre capabilities also aided Ukrainians a lot.

Nevertheless, the Russians used their mass to continue to move forward. However, by the time they took control of Hostomel airport and other objectives to start attacking Kyiv, they lost the momentum and the required combat power to seize such a large and complex target successfully. While encircling the capital, they were stretched even more thin and thus became more vulnerable to raiding (Watling, 2022). Ukrainian attacks in the rear also forced Russians to redirect a substantial portion of their formations to defend main supply lines, thus reducing the possibility of attacking Kyiv. Berkowitz (2022) summarised the main Russian problems: 'scattered command structure, lack of convoy protection, shortages of critical supplies, questionable medical care, not enough guided missiles, excessive vehicle breakdowns'.

UASOF very effectively utilised the main principles of doctrinal DA operations. By using special skills, special techniques (highly manoeuvrable small-sized units), special equipment (specifically the night and thermal vision capability) and a synthesis of accurate intelligence (coming from various sources like foreign military support, national security agencies, local citizens, and others) they succeeded in gaining a relative advantage against sounder adversary and inflicted damage that later proved to be of strategic importance. UASOF also intensely utilised support from other services – specifically Artillery and Air Force – by providing target information to execute terminal guidance and precision destruction operations. To multiply the effects, many of these operations were recorded and later used for informational campaigns by UASOF's psychological operations units. The enemy was forced to reduce the capabilities of offensive operations to prevent attacks on its rear logistical units. All of these achievements, in conjunction with efforts of other military services and governmental institutions, set conditions for the most critical strategic victory – securing the capital, Kyiv, forcing the enemy to abandon the initial campaign plan and retreat from northern Ukraine.

The existing doctrinal descriptions have mainly derived from a long history of SOF raids on violent extremist organisations (VEO) in Iraq and Afghanistan to destroy their

networks through continuous night assaults. Even though VEO networks showed remarkable resilience, which proved this tactic inefficient (Jones, 2020), this was not the case in a state-to-state conflict. Russian hierarchical command structure proved to be very susceptible to the removal of key individuals. Notably, AJP-3.5 SOF activities within the Allied Joint operations do not describe such use of SOF but instead focus on counterinsurgency, counterterrorism, countering hybrid threats, countering the proliferation of weapons of mass destruction, hostage release operations, and faction liaison (NATO, 2019). However, UASOF, by being part of the joint defensive operation against an initially stronger opponent, proved otherwise.

2.2. Special reconnaissance: threat & target assessment and post-action reconnaissance behind enemy lines.

Russians did not listen to the wise words of Omar Bradley, the USA general during the Second World War, who once said, 'Amateurs talk strategy, and professionals talk logistics'. It eventually became one of the most significant vulnerabilities of the initially planned Russian *blitzkrieg*. Per the battle for Kyiv, logistical factors established constraints to the possible operational courses of action. Loss and disturbance of logistical supply disabled the force's capability to manoeuvre, degraded initiative and morale, and even incapacitated the combat power due to the simple lack of ammunition and fuel (Watling, 2022). Eventually, resources diverted from the main line of effort imposed operational and strategic defeat.

Such circumstances provided an impeccable opportunity for small and manoeuvrable UASOF units to penetrate behind enemy lines in temporarily occupied and enemy-owned territory and impose pressure on main supply routes, logistical hubs, warehouses, convoys, and critical infrastructure (Dieanu, 2022). While having limited organic firepower, UASOF units provided threat and target assessment to create a sufficient relative certainty for indirect fires or air-delivered munition strikes. SOF-delivered post-action reconnaissance also played a crucial role in gathering information for battle damage and operational assessment to evaluate the results of military action applications. As part of the intelligence collection process, UASOF utilised various intelligence disciplines like unmanned aerial vehicles, visual target surveillance and especially the local population, which became one of the key informants of the Ukrainian military (Watling, 2022). Due to extreme hostility towards Russian occupiers, an extensive human intelligence network throughout the war has

made a crucial contribution to the long-range precision fire targeting process (Watling et al., 2023). This is a real-life example where SOF's emphasis on relationships and the ability to build networks played a crucial and substantial role (Taft et al., 2019).

Dieanu (2022) considers that UASOF proved their operational capability by executing these types of missions in all sorts of hostile territories (both Ukraine and Russia), seizing low visibility opportunities at night or under unfavourable weather and terrain conditions. To achieve this, UASOF had to be adaptable, rapid, and skilled in reaching high levels of accuracy against peer adversaries. Small and substantially mobile teams must have had flawless decision-making and situational awareness processes ensured by an uncompromised level of secure connectivity. Only networked and empowered teams could have been able to conduct SR tasks in identifying targets for deep fires or even striking independently (White, 2022b). For later cases, UASOF was equipped with effective, lightweight, highly mobile precision-guided loitering munitions and man pads. Loitering munitions proved themselves to be a very prolific solution which provided SOF teams with the organic capability to conduct beyond-line-of-sight surveillance and reconnaissance of potential targets and to execute hit-and-run attacks, engaging them at a very concise timeframe (White, 2022b). Once again, the use of special training and special equipment demonstrated its value. Night vision goggles, FLIR radars, innovative weapon systems, all-terrain light vehicles, boats, access to airframes and unmanned combat aerial vehicles, and other special equipment proved to be efficient not only in airspace-dominated environments like Iraq or Afghanistan but also in a peer-to-peer conflict (White, 2022a).

The doctrinal framework of SR references operations in hostile or denied environments to collect or verify information of strategic or operational significance by using distinct capabilities, techniques, and modes of employment. That is precisely what UASOF did from the first days of the invasion throughout the whole war period to date. SOF units infiltrated Russian territory and continued to provide vital information for the joint targeting process. The role of CS assets like unmanned drones, electronic and cyber warfare, satellite communications, and other technological developments inevitably gained an increasingly substantial role in such forms of warfare. In contrast, AJP-3.5 speaks concisely of CS and suggests only a possible requirement of such capabilities.

Operations in hostile territories behind enemy lines require SOF units to be highly self-sustainable and self-dependent. If those units over-rely on external support or require constant endorsement and guidance from higher command, they cannot perform up to expectations. That not only requires a very specific type of equipment, but mostly, it depends on a human factor – selected and specially trained operators who can be trusted to perform independently and sometimes even single-handedly. That also calls for a certain mind shift in all levels of command and doctrinal approaches to distinctive SOF nature after long years of operating against VEOs in comfortably matured battlegrounds. All this effort presents specific deep battle options to create operational or strategic dilemmas for the adversary.

2.3. Military assistance: organisation of the resistance network in temporarily occupied areas.

On the eve of the Russian full-scale invasion, in January 2022, Ukraine's legislative body introduced a National Resistance Strategy, where UASOF was tasked with preparing a national resistance campaign (Danylyuk, 2023). While still in the transformation process, UASOF received an additional assignment to spearhead a resistance movement in temporarily occupied territories if such a situation arose (Dieanu, 2022). Ukraine's political and military leadership set a legal framework and organisational structure to implement a broad whole-of-society total defence, including SOF, as part of the planning and preparation process. Armed resistance, in the form of insurgency, was introduced as a part of the more extensive conventional warfare, where it could provide necessary disruption of the enemy's rear lines of supply or communication and drain its forces from the main battlefield (White, 2022b).

In theory, SOF is one of the two critical components for a concept of effective total defence alongside a voluntary-based, citizen-soldier manned territorial defence force (TDF). Stringer (2022) proposes a few SOF and TDF collaboration models – the force provider opportunity, the training and doctrine possibility, and the advice, assist, and accompany option. Most importantly, this instrument must be established, coordinated and well-prepared early in peacetime. Pettersson (2022) suggests that such measures could provide additional tools to resist an occupying force and possibly win a war by not losing it.

During the early stages of the war, UASOF established the National Resistance Centre to train, coordinate, and support resistance movements. Information on possible resistance concepts was provided on open-source channels (Hogue, 2023). Various sources, including interviews with privileged UASOF operators, prove that UASOF succeeded in providing MA and integrational functions to resistance and sabotage activities (Borsari, 2023). After February 2022, a part of the territory of Ukraine, together with a sizable number of Ukrainian citizens, was temporarily occupied (Pettersson, 2022). The general acceptance of Russians was very low, so the resistance movement grew exponentially. Some people tried to organise peaceful demonstrations, but arrests, beatings, and extortion swiftly eradicated those. Since then, the primary role of the resistance movement in the temporarily occupied territories has been the gathering and transmission of various intelligence information – especially the location of all sorts of military objects and post-strike assessments (Danylyuk, 2023). Visually recorded post-strike assessments were widely used in a broad messaging campaign to boost Western support and improve the morale of the internal audience. Moreover, this information is used as evidence to analyse, expose, and prosecute war crimes committed by the Russian army (Hogue, 2023).

The irregular warfare operations in eastern Ukraine brought instability by affecting the enemy's morale. They delayed occupational actions or even led to the Russian withdrawal from some areas. Quite a substantial number of cases of railway system disruption in Ukraine, Russia, and Belarus by incapacitating locomotives, destroying parts of railways, or burning the relay sections caused delays in material supplies, machinery, and personnel (Danylyuk, 2023). A series of precision DA assaults conducted with the support of the UASOF annihilated a substantial number of Russian high-ranking officials and local administration marionettes, significantly diminishing the capabilities of the extraordinarily hierarchical and inflexible Russian command structure (Dieanu, 2022).

Although insurgency rarely presents quick victory, modernisation, innovation, and abundant digital technologies enabled UASOF to change the resistance network's nature and tasks considerably, especially in a state-to-state conflict. With the availability of long-range weapons, risky kinetic operations became a less preferred option. With the internet, social networks and digital media availability, psychological operations could be conducted from remote, safe locations. Physical participation in

protests and peaceful demonstrations was ineffective against a neglectful opponent like Russia. However, Ukrainian resistance networks proved highly effective in intelligence collection, target acquisition and small-scale but effective sabotage operations. That type of mission set required robust, compartmentalised, disguised, and undetectable communication channels to exchange information, protect users, and, at the same time, provide contribution options for any willing informant. Moreover, Russian procedures of human terrain mapping and the ability to conduct targeting against resistance networks via penetration into governmental structures required a networked approach to the resistance organisation rather than having a hierarchical and structured body led by UASOF operators.

Conclusions and recommendations.

The Russo-Ukrainian war is the first in recent history where SOF units conduct high-intensity combat actions against a peer adversary. This research confirmed that UASOF, trained and equipped according to NATO standards, by executing SOF doctrinal core tasks, demonstrated SO warfare's operational power and ability to carry out successful missions of operational and strategic value. Case studies showed that all three SOF principal tasks found their place on this particular battlefield, proving that SOF doctrinal core tasks remain the essence of the special operations warfare but should be reviewed and updated regarding SOF's role, types of operations, and required equipment in a state-on-state military conflict environment. The basis of NATO SO warfare – the AJP-3.5, is an output of over twenty years of counterterrorist and counterinsurgency campaigns in the Middle East with different battlefield maturity levels, but almost always with air supremacy present. Subsequently, it is mainly expeditionary and offensive-centric. Thus, it does not incorporate the application of SOF in homeland defence. That would not be the case in a state-to-state conflict, where SOF support for joint warfare would be of primary importance. The analysis throughout this research project led to the recommendations provided in the following paragraphs.

The main principles of doctrinal DA operations proved adequate for gaining a relative advantage against peer state-level adversaries and enabling SOF to reach the required effects upon objectives of strategic significance. As part of joint defensive or counter-offensive operations, SOF could provide preciseness, skill, and clandestine

approaches in highly restricted environments. That requires a revision of the AJP-3.5 description of SOF activities within the allied joint operations, which does not portray such use of SOF at this time.

The doctrinal framework of SR operations remains vital to success throughout the whole spectrum of competition, crisis, and war. SOF units are trained, equipped, and enabled to infiltrate hostile, enemy-controlled territory and provide vital information for joint targeting. However, the importance of modern CS in such types of SO is exponentially growing. Highly sophisticated CS assets should be introduced as organic SOF structural elements. This should be implemented at all levels, from the Special Operations Component to the Special Operations Task Unit, with an expansion of the current order of battle, appropriate integration and adequate training. Experience gained in the ongoing war should be thoroughly reviewed and introduced into the doctrinal spectrum of SO warfare alongside more frequent doctrine revisions to keep up with the tempo of technology developments.

State-to-state conflict could be very asymmetric in the opponents' diplomatic, informational, military, and economic strength. Although insurgency rarely presents quick victory, sometimes such a method of unconventional warfare might be an imposed choice for smaller states. With technological modernisation, the resistance networks could be highly effective in intelligence collection, target acquisition and small-scale but effective sabotage operations. The effects of these operations could be effectively multiplied by the application of psychological operations. Resistance and resilience network operations should become an intrinsic task for SOF units, and the approved Resistance Operating Concept doctrine should be aligned with or even integrated into AJP-3.5 to make the doctrine more universal and to provide necessary tools for early planning, preparation, and execution of state-internal MA.

Historically, SOF played a relatively minor but certainly substantial role in major power deterrence and conflict. Nowadays, SOF can uniquely create a new, powerful form of unconventional deterrence, supplementing the traditional and nuclear ones. NATO SOF units can have confidence in doctrinal special warfare and that their tactics, training, and equipment are adequate for contemporary challenges. As per SOF's motto – improvise, adapt, overcome – units must be ready to use customary techniques and hybrid approaches based on advanced technologies. Only self-

enabled, self-sustainable and self-dependent SOF units under a robust mission command approach of C2 principles would be able to provide deep battle options. Since war is ongoing, new information and freshly gained experience can always pop up due to the developments on the battlefield. Undoubtedly, the future of SO warfare and the organisation of SOF within NATO countries will be significantly shaped by analysing the UASOF role in the Russo-Ukrainian war.

Abbreviations.

AJP-3.5 – NATO Allied Joint Publication 3.5: Allied Joint Doctrine for Special Operations

C2 – Command and Control

CS – Combat Support

CSS – Combat Service Support

DA – Direct Action

ISR – Intelligence, Surveillance and Reconnaissance

MA – Military Assistance

SO – Special Operations

SOF – Special Operations Forces

SR – Special Reconnaissance

TDF – Territorial Defence Force

UASOF – Ukrainian Special Operations Forces

VEO – Violent Extremist Organisation

Bibliography.

Berkowitz, Bonnie and Galocha, Artur. 2022. Why the Russian military is bogged down by logistics in Ukraine. Washington Post. [Online: 30 March 2022]. [Cited: 31 August 2023]. <https://www.washingtonpost.com/world/2022/03/30/russia-military-logistics-supply-chain/>

Borsari, Federico. 2022. Hunting the Invader: Ukraine's Special Operations Troops. Cepa. [Online: 15 March 2022]. [Cited: 27 August 2023]. <https://cepa.org/article/huntingthe-invader-ukraines-special-operations-troops>

Borsari, Federico. 2023. Ukrainian Special Forces – Preparing the Battlefield. [Online: 22 May 2023]. [Cited: 27 August 2023]. <https://cepa.org/article/ukrainian-special-forces-preparing-the-battlefield>

Borsuk, Arthur. 2023. Russia-Ukrainian War 2022: Battle of Hostomel. Old Dominion University Graduate Research Conference. [Online: 10 February 2023]. [Cited: 23 August 2023]. https://digitalcommons.odu.edu/gsis_studentconference/2023/ukrainianresilience/4/?utm_source=digitalcommons.odu.edu%2Fgsis_studentconference%2F2023%2Fukrainianresilience%2F4&utm_medium=PDF&utm_campaign=PDFCoverPages

Collins, John. 1987. United States and Soviet Special Operations. Report for US Congress. [Cited: 12 October 2023].

Danylyuk, Oleksandr. 2023. Against the Odds: Lessons from the Ukrainian Resistance Movement. Rusi. [Online: 4 July 2023]. [Cited: 27 August 2023]. <https://rusi.org/explore-our-research/publications/commentary/against-odds-lessons-ukrainian-resistance-movement>

Dieanu, Adrian-Corneliu. 2022. The Role of Ukrainian Special Operations Forces within the War in Ukraine. Carol I, the National Defence University of Bucharest. [Online: 28 July 2022]. [Cited: 27 September 2023]. <https://www.ceeol.com/search/chapter-detail?id=1120550>

Hogue, Simon. 2023. Civilian Surveillance in the War in Ukraine: Mobilizing the Agency of the Observers of War. Surveillance & Society. [Online: 16 March 2023]. [Cited: 27 September 2023]. <https://ojs.library.queensu.ca/index.php/surveillance-and-society/index>

Hooker, D. Richard, Jr. 2023. America's Special Operations Problem. Joint Force Quarterly. Volume 108, 1st Quarter 2023. [Cited: 30 August 2023]. <https://ndupress>.

ndu.edu/Portals/68/Documents/jfq/jfq-108/jfq-108_50-55_Hooker.pdf?ver=_ZQUsAccke1T_D0ipKBmbQ%3d%3d

Jones, Grace, Egan, Janet and Rosenbach, Eric. 2023. Advancing in Adversity: Ukraine's Battlefield Technologies and Lessons for the U.S. Policy Brief, Belfer Center for Science and International Affairs, Harvard Kennedy School. [Online: 31 July 2023]. [Cited: 30 August 2023]. <https://www.belfercenter.org/publication/advancing-adversity-ukraines-battlefield-technologies-and-lessons-us>

Jones, Robert C. 2020. Conceptualizing the Future of US Special Operations. Small Wars Journal. [Online: 11 April 2020]. [Cited: 30 August 2023]. <https://smallwarsjournal.com/index.php/jrnl/art/conceptualizing-future-us-special-operations>

Joint Special Operations University (JSOU). 2023. Special Operations Forces Reference Manual (fifth edition). [Online: 11 January 2023]. [Cited: 30 September 2023]. <https://jsou.edu/Press/PublicationDashboard/240>

McRaven, William H. 1996. Spec Ops: Case studies in Special operations warfare: theory and practice. New York, NY: Ballantine Books. [Cited: 30 October 2023].

Momi, Rachele. 2022. Ukrainian Special Operations Forces (UASOF). Grey Dynamics. [Online 25 October 2022]. [Cited: 30 August 2023]. <https://greydynamics.com/ukrainian-special-operations-forces-uasof/>

NATO. 2019. NATO Allied Joint Publication. AJP-3.5: Allied Joint Doctrine for Special Operations. Edition B Version 1. [Cited: 30 August 2023].

NATO. 2022. Madrid Summit Declaration. 29 June 2022. [Cited: 25 August 2023]. https://www.nato.int/cps/en/natohq/official_texts_196951.htm

NATO. 2023. Vilnius Summit Communiqué. 11 July 2023. [Cited: 25 August 2023]. https://www.nato.int/cps/en/natohq/official_texts_217320.htm?selectedLocale=en

Pettersson, Ulrica and Ilis-Alm, Hans. 2022. Resistance Operations: Challenges and Opportunities for Special Operations Forces. Journal on Baltic Security. 2022, 8 (1). [Online 25 May 2022]. [Cited: 25 August 2023]. DOI: 10.57767/jobs_2022_0009

Sanders, Deborah. 2023. Ukraine's third wave of military reform 2016–2022 – building a military able to defend Ukraine against the Russian invasion. Defense & Security Analysis. [Online 4 June 2023]. [Cited: 25 September 2023]. DOI: 10.1080/14751798.2023.2201017

Sof, Eric. 2012. Special Forces and their role in the history of warfare. Spec Ops Magazine. [Online 15 October 2012]. [Cited: 25 August 2023]. <https://specialops.org/special-forces-in-history-of-warfare/>

Solli, Bjorn-Erik. 2021. The essence of Special Operations (What you need to know about Special Operations while serving at the Joint Operational level). Norwegian Special Operations Command, Special Operations Advisor to NATO Joint Warfare center. [Online 5 October 2021]. [Cited: 30 August 2023]. <https://www.stratagem.no/the-essence-of-special-operations>

Special Operations Forces of the Armed Forces of Ukraine. 2016. Tasks of the Special Operations Forces of the Armed Forces of Ukraine. [Cited: 30 August 2023] <https://sof.mil.gov.ua/>

Stojar, Richard. 2023. The Russian invasion and its failure in the first days. Defense & Security Analysis. 39:3, 296-311. [Online 26 July 2023]. [Cited: 30 August 2023]. DOI: 10.1080/14751798.2023.2232188

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). [Online 3 October 2022]. [Cited: 30 August 2023].

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). A report from the Deloitte Center for Government Insights. [Online 2019]. [Cited: 30 August 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 August 2023]. https://www.militairespectator.nl/sites/default/files/teksten/bestanden/militaire_spectator_2_2021_titulaer.pdf

Unian. 2019. Ukrainian spec-ops forces unit passes NATO certification, first time in history. [Online 24 June 2019]. [Cited: 29 August 2023]. <https://www.unian.info/politics/10595037-ukrainian-spec-ops-forces-unit-passes-nato-certification-first-time-in-history.html>

USA Department of Defence. 2020. Joint Publication 3-05 Joint Doctrine for Special Operations. [Cited: 29 August 2023].

USA Department of the Army. 2024. Army Techniques Publication No. 7-100-1 Russian Tactics. [Cited: 11 March 2024].

USA Special Operations Command Europe. 2019. Resistance Operating Concept. [Cited: 29 February 2024].

Verkhovna Rada. 2016. Law of Ukraine on the Special Operations Forces of the Armed Forces of Ukraine. Bulletin of the Verkhovna Rada, 2016, No. 33. [Cited: 29 December 2023].

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 August 2023]. https://static.rusi.org/whr_special_forces.pdf

Watling, Jack and Reynolds, Nick. 2022. Operation Z: The Death Throes of an Imperial Delusion. Rusi. [Online 22 April 2022]. [Cited: 30 August 2023]. <https://rusi.org/explore-our-research/publications/special-resources/operation-z-death-throes-imperial-delusion>

Watling, Jack, Danylyuk, Oleksandr and Reynolds, Nick. 2023. Preliminary Lessons from Russia's Unconventional Operations During the Russo-Ukrainian War, February 2022–February 20. Rusi. [Online 29 March 2023]. [Cited: 25 August 2023]. <https://static.rusi.org/202303-SR-Unconventional-Operations-Russo-Ukrainian-War-web-final.pdf.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. [Online 15 December 2016]. [Cited: 25 September 2023].

White, Andrew. 2022a. Ukraine conflict: Ukrainian Special Operations Forces in focus. Janes. [Online 4 March 2022]. [Cited: 25 August 2023]. <https://www.janes.com/defence-news/news-detail/ukraine-conflict-ukrainian-special-operations-forces-in-focus>

White, Andrew. 2022b. Europe's special operators are watching Ukraine closely for lessons learned. Breaking Defense. [Online 29 April 2022]. [Cited: 30 August 2023]. <https://breakingdefense.com/2022/04/europes-special-operators-are-watching-ukraine-closely-for-lessons-learned/>

Wilk, Andrzej. 2017. The best army Ukraine has ever had. Centre for Eastern Studies. Number 66. [Online 2017]. [Cited: 30 October 2023]. <https://www.ceeol.com/search/book-detail?id=836062>

KEVIN TEULADE. Russian Information Warfare in Estonia – A Case Study

How can a cheese sausage be turned into a weapon of information warfare? Zoja Paljamar, a Russian propagandist expelled from Estonia last June, has recently been exposed by Facebook users and the Propastop (Propastop, 2023), a volunteer-based fact-checking website linked with the Estonian Defense League (*Kaitseliit*). Zoja Paljamar had posted a picture of Rakvere (Estonian meat producer) products being allegedly sold in a Saint Petersburg store. She had added a caption saying "Discovered in St. Petersburg supermarket. How is that? Where are the sanctions?". The post aimed to convey that the Western-imposed sanctions on Russia are ineffective. The takeout from this case is that any benign information can be weaponized. Information is a prominent battlefield in the Ukraine war and the broader influence contest Russia imposes on what it refers to as "the West" (Diligenski, 2001).

Propaganda, psychological warfare, influence operations, information confrontation. There are many confusion (Herb, 2020) in military thought and academic papers to qualify Russian manipulation of information. This article will employ the term "information operations" (InfoOps) to address those operations. InfoOps are defined by the United States as:

[the] integrated employment, during military operations, of information-related capabilities in concert with other lines of operations to influence, disrupt, corrupt, or usurp the decision making of adversaries and potential adversaries while protecting [its] own (Department of Defense, 2017).

It is a subclass of influence operations, that also encompass diplomacy, strategic communication, and covert operations (Hutchinson, 2010). Psychological operations (PSYOPS) are even broader. According to the US doctrine, PSYOP are:

selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign

governments, organizations, groups, and individuals in manner favorable to the originator's objectives¹ (Herb, 2020).

There is an extensive literature describing Russian strategies and concepts. In this article, terms and concepts used will be those commonly employed by NATO countries. The author hopes this choice will help give a different insight into the Russian approach by presenting its strategy through the use of Western concepts.

In adopting the expression "information operation", this article wants to analyse Russian influence as nonlinear part of a broader military campaign aiming to disrupt the rule-based international order (RBIO). This paper uses the Estonian democracy as a case study. Estonia had been forcibly integrated into the Soviet Union, thus being a de facto Soviet Socialist Republic (SSR) from 1940 until 1991. Occupation resulted in mass Russian-speaking immigration. Estonia has since turned into a vibrant European democracy. It makes is henceforth a relevant case to analyse the strengths and weaknesses of a former SSR with a Russian-speaking minority turned into a European Union (EU) democracy and North Atlantic Treaty Organisation (NATO) member.

The case study will be conducted through the qualitative analysis of three different InfoOps that occurred no later than five years ago: the Impressum Club activities, COVID-19-related narratives, and the Russian influence over certain political parties. This paper will assess Estonia's vulnerability to InfoOps, trying to identify the objectives pursued and methods employed by the Russian Federation (RF).

The expected outcome of this study is to understand better the Russian objectives and patterns in Estonia and how to address them in a democratic context. This paper argues that the Estonian democracy is vulnerable to RF InfoOps as they threaten to fracture societal cohesion in Estonia, which is vital to the country's security (Prause, Tuisk, and Olaniyi, 2019).

This paper will first analyse the Centres of Gravity (CoGs) of the Estonian society that could be of interest in the structuring of hostile InfoOps. Then, it analyses the Russian

¹ "JP 3-13.2 replaced the term PSYOP with MISO to 'more accurately reflect and convey the nature of planned peacetime or combat operations activities.' The name change reportedly caused administrative confusion, and the services are beginning to revert to the PSYOP label" (Theohary, 2020).

interests in Estonia and attempts to build a typology of InfoOps according to Russian records and doctrine in this area. Once Estonian CoGs and Russian objectives and likely Courses of Action (CoAs) are established, the case studies will be analysed through this framework. Finally, this paper elaborates on the current counterstrategies implemented.

THE ESTONIAN SOCIETY

Eastern Europe, since the collapse of the Soviet Union, faces the issue of building or rebuilding nation-states. In the case of the Baltic states, the construction of national identities is rendered difficult by the proximity of a neighbour as giant as Russia, compared to their relatively small population and territory.

While the definition of the term “nation” is an open academic debate, this article uses Brubaker’s classic definition (Petersoo, 2007). A nation comprises a group of citizens exerting their right of self-determination within a territory. Hence, it requires the will of a majority to live together and the reconnaissance and respect of minorities within its boundaries (Brubaker, 1996). Brubaker’s definition of the legitimacy of a nation can be challenged by the classic triptych of legitimacy established by Max Weber (Lottholz and Lemay-Hébert, 2016). According to the German scholar, legitimacy can be sourced from tradition, legality, or charisma. Under the legality paradigm, the Estonian state’s existence is noticeably rooted in its recognition by the international community. Russia was one of the first countries to acknowledge its reacquired independence. However, good relations did not last long. The 1993 Citizenship law based attribution of nationality on Estonian language proficiency. This decision resulted in a significant part of Soviet time settlers and their offspring not acquiring Estonian citizenship. It created the first strife between Tallinn and Moscow. The pending ratification of the Estonian–Russian border treaty is another source of tension.

The Estonian society, since the country’s reaccession to independence in 1991, has adopted democratic and liberal values, and shifted its focus towards the Western world. First, Estonia is an increasingly liberal pluralist parliamentary democracy. Three traits strongly differ from the path Russia has embraced since the collapse of the USSR. The Estonian Constitution establishes the country as a democratic republic, with a thorough system of checks and balances. Noticeably, the role of the President, inherited from the third constitution, is maintained but with an honorary role. The institutional heart of the Republic lies in the *Riigikogu*, a unicameral parliament (*Riigi*

Teataja, 2024). The model built by Kersnauskaite (2022) to analyse Estonians' feelings about democracy reports a solid will to maintain democracy, even though it also depicts dissatisfaction with the current institutions. The support is significantly higher compared to Western states that have not experienced an authoritarian regime within the lifespan of a generation.

Beyond being committed to their democratic institutions, Estonians do involve themselves in the electoral process. General and local elections since 1992 have consistently shown relatively constant and positive participation rates² (*Valimised*, 2024). Even though internet voting was not the game changer some expected it to be (Toots, 2019). The number of candidates has remained steady, with an average of 1.050 candidates at the general elections and 13.000 candidates at local elections (1% of the population). The multiparty system is supported by the proportional voting mode applied in the general elections. However, membership in parties has receded in recent years, except for the Conservative People's Party of Estonia, EKRE (*Eesti Konservatiivne Rahvaerakond*) (Kersnauskaite, 2022). Main Estonian parties have endured time since the early 2000s (Auers, 2018), with regular new offer also appearing (EKRE, *Eesti 200*).

Estonia can also be considered as a liberal society. The Estonian successive governments in the 1990s sought swift access to the European Union, which it achieved through the implementation of a political agenda that Kamerade calls "Europeanisation" (Kamerāde, Crotty, and Ljubownikow, 2016). It resulted in the development of civil liberties and a dramatic increase in nongovernment organisations and volunteer work. However, the emergence of EKRE in the public debate emphasises a growing dissent of a significant proportion of the population with the democratic liberal paradigm (Ploom, Sazonov, and Foster 2023). In the two latest general elections, EKRE secured nearly 18% (2019) and 16% (2023) of the popular vote (*Valimised*, 2024). It advocates for a tight migration policy and plays on cultural insecurity (Makarychev and Sazonov, 2019). The development of a strong democracy with various ways for the citizens to participate in public life has significantly contributed

² Between 57,4% (1999) and 68,9% (1995) of total registered voters.

to Estonia moving away from Russian influence. In addition, this adherence to democracy exposed Estonia to Western influence.

Adhering to the European Union and the North Atlantic Treaty Organisation (NATO) brought significant changes in the Estonian political and diplomatic orientation, economy and culture, and use of languages within the country. It resulted in a dramatic increase of diplomatic ties with Western capitals along with a thorough review of national interests to integrate European and Alliance goals (Lawrence, 2023), which further alienated Estonia from Russia's influence. As a result, Estonia's economic and cultural relations shifted towards the West. Between 2008 and 2014, there was a sharp increase in economic exchanges with EU members (Raudjärv, 2015). Through the study of luxury goods consumption, Polese and Seliverstova (2020) show conscious and widespread consumer choices favouring Western-style options. However, it can be noted that even though the economic relations with Russia decreased in proportion, their level remained high. Similarly, the Russian-speaking population in Estonia did not adopt Western-oriented consumption choices.

However, the use of languages across the country reveals the societal divisions with the most accuracy. When Estonia reclaimed its independence, the nation-(re)building strategy emphasised the Estonian language as the main attribute of "Estonianness" (Oskolkov, 2023). As a result of the decision of the Estonian Supreme Council of February 26, 1992, to restore the 1938 Citizenship Act and consider that every decision taken from June 16, 1940, was *ex tunc* invalid, the Russian-speaking population who had settled down in the country from this date on, and their offspring, found themselves stateless. As of 2019, 72,400 people of undetermined citizenship reside in Estonia (Siseministeerium, 2024). However, the Russian-speaking minority in Estonia instead represented, according to the 2021 Statistics Estonia census, 29% of the Estonian population (Statistikaamet, 2022), or approximately 386,000 people. Speaking Russian as a mother tongue does not align with Russian origin. It encompasses other ethnicities from the former Soviet Union. Nevertheless, it still represents a good estimation, and the census has been conducted prior to the Russian aggression of Ukraine and subsequent Ukrainian refugees' migration to Estonia. Another noticeable outcome of this census is that English as a foreign language is now better known and used than Russian in Estonia. In ten years, the Estonian population changed its language preferences as it turned its interest westward.

The Russian-speaking minority's (hereafter referred to as EST-RUS) perception of the social environment it lives in stands out from the ethnic Estonians (EST) (Teperik, 2023). Their level of confidence in the government, their perception of safety and their economic perspectives are consistently lower than EST (Teperik, 2023; Trifonova, 2021). This rift in Estonian society is perceived by some as a vulnerability (Kallas, 2021).

To summarise, Estonian society is democratic and liberal and has been culturally turning westward quickly and resolutely. The CoGs of the Estonian Society are, as discussed above:

- CoG1: A functioning parliamentary democracy.
- CoG2: An engaged, liberal society.
- CoG3: Western-oriented national ethos.
- CoG4: A language-based national identity.

However, two vulnerabilities can be identified: its conservative Europhobic political movement and its EST-RUS minority, which is partially integrated. Such vulnerabilities are easy targets for Russia's information operations.

RUSSIAN INFORMATION OPERATIONS

To understand the threat Russia poses, it is first necessary to assess Russian objectives. According to Dikij (2016), the "Russian world" ("*Русский мир*") breaks down into four concentric circles. The Russian Federation is under the Kremlin's direct, "vertical" authority. The second layer consists of former Soviet Socialist Republics (SSRs), with Moscow seeking to control their foreign policy, military, and intelligence services. The ideal-type former SSR for Moscow is Belarus. The country, run by a puppet government, is bound by political, military, and commercial agreements, transferring most of its authority to the Russian Federation (RF). It is an undemocratic state, culturally oriented towards Russia. Armed forces and intelligence services officials are Federal Security Service (FSB) or Main Directorate of the General Staff of the Armed Forces (GRU) relays of influence. The third circle comprises the former Warsaw Pact allies, Balkan region countries, and several third-world countries, including Syria, Mali, Iran, India, and Brazil. Controlling those states is regarded as impossible by the Kremlin. Its main goal is achieving systematic support in foreign relations feuds with the Anglo-Saxon world. The last circle is Western continental

Europe, from the Scandinavian states to Spain, which Russia sees as a necessary buffer to insulate the Russian World from its archenemy. In this area, Russia aims to sedate opposition through economic dependence and corruption.

Henceforth, it can be argued that the RF Political Objectives³ (POs) are:

- **PO1:** Undisputed authority of the Kremlin within the RF.
- **PO2:** Control over the foreign policy, military, and intelligence service of former SSRs.
- **PO3:** Prevalence over the Anglo-Saxon bloc in International Relations through secured support of former Warsaw Pact and Global South States.
- **PO4:** Neutrality of Western continental Europe.

This vision may appear as *delirium*. It is unfortunately an effective grid to analyse Russian aims in respective countries.

Disregarding the resources it would take Russia to achieve its vision, two geopolitical realities prevent its implementation: NATO and the EU. As demonstrated *supra* with the Estonian case, the EU dragged away Central and Eastern European (CEE) countries from Moscow's soft power. At the same time, NATO protects them against the Kremlin's tendency to use hard power when its influence decreases. To achieve its **PO2** and **PO4**, Russia's strategic objectives are neutralising the EU and NATO. It is then no surprise that Eurosceptic parties are, in one way or another, backed by Moscow (Hankewitz, 2023; Turchi, 2023).

- **SO:** Neutralising the EU/NATO.

Whether or not Russia's *grand plan* may be achieved, the wars in Georgia, Syria, and Ukraine, or the military intervention in Kazakhstan, show that the Kremlin is seizing opportunities to implement its vision locally. Strategic advantage can be gained from partial successes, such as Abkhazia to Georgia or Crimea to Ukraine.

Estonia is a former SSR, with, as discussed *supra*, one-third of EST-RUS. According to the Russian vision, Estonia should be as much a puppet state as Belarus is. The

³ An analysis of the Russian Foreign Policy Concept concurs to this vision - (Министерство иностранных дел Российской Федерации, 2023а)

Soviet occupation of Estonia resulted in mass economic migrations of Russians in Estonia (Aidarov and Drechsler, 2013). However, Estonia moved away from Soviet and then Russian influence very early after the collapse of the Union, and in vigorous terms. The abovementioned decision of Estonia to consider the Soviet era as an occupation was a bold statement in its foreign relations, strongly contradicting the Russian conception of former SSRs as its area of influence.

The Kremlin understands the grammar of article 5. Its operational design adapts to reality. On the Russian World board, some of the second circle countries cannot be coerced into doing the Kremlin's will through force, being protected by the North Atlantic Treaty. Thus, Moscow resorts to alternative strategies. Such strategies may be economic, diplomatic, cultural, or informational (Nye, 1990).

To achieve its political and strategic goals in Estonia through unconventional means, Russia needs to attack the country's CoGs. Russian operational objectives in Estonia are thus:

SO: Neutralising the EU/NATO.	
Theatre SO: Break Estonia apart from EU and NATO.	
CoG1: A functioning parliamentary democracy;	OO1: Disrupt / Neutralise the democratic process in Estonia.
CoG2: An engaged, liberal society;	OO2: Disrupt / Neutralise Estonian societal cohesion.
CoG3: Western-oriented national ethos;	OO3: Influence the Estonian audiences against the West, in favour of the RF.
CoG4: A language-based national identity.	OO2: Disrupt / Neutralise Estonian societal cohesion.

Table 2. Strategic and Operational Russian Objectives against Estonian Centers of Gravity. Source: Author's own. Within the Kremlin's arsenal, non-lethal operations are grouped under the Information Confrontation umbrella (Arold, 2016). Propaganda is deeply rooted in Modern Russia and finds its roots in the Soviet political warfare tradition (Smith, 1990). The Soviet-based Active Measures framework can be updated to build a modern typology of Russian Information Operations (noted as IOMEs, standing for Information Operation Mode of Action of the Enemy):

- **IOME1:** Disinformation (across the information domain⁴).
- **IOME2:** Use of media/expert audience in targeted countries.
- **IOME3:** Use of political parties and non-governmental organisations (NGOs) abroad.
- **IOME4:** Use of social media to shape the information sphere.

CASE STUDIES OF RUSSIAN INFOOPS IN ESTONIA

The two previous chapters aimed to establish the CoGs of Estonia, the Russian objectives, and their MEs in the information field. The present case studies demonstrate how the IOMEs can support RF objectives in Estonia. The following three cases represent different IOMEs: COVID-19 disinformation (IOME1/2/4), the *Impressum* Case (IOME2), and how EKRE plays for Russia (IOME3).

How did Russia contribute to COVID-19 conspiracy theories, and how did they influence security in Estonia?

Undermining the society's resilience is a Russian Operational Objective in Estonia (OO2, cf. infra). Conspiracy theories constitute a weapon of choice as they favour social dissent and belief in other conspiracy theories. Astapova (2023) demonstrated that in Estonia, non-vaccinated individuals are more likely to support the Russian invasion of Ukraine, thus establishing a correlation between belief in conspiracy theories and support to Russian narratives.

In 2020, as concerns regarding the coronavirus brought entire countries to lockdown, another pandemic spread worldwide. World Health Organization (WHO) Director-General Tedros Adhanom aptly referred to this phenomenon as an "infodemic" (Simon and Camargo, 2023). The pandemic triggered a wave of distrust against wavering political decisions. Alternative channels of information trended, such as social networks, often displaying foreign influence. Out of 386 disinformation narratives attributed to Russia identified by the European External Action Service (EEAS) operated EUvsDISINFO platform (EUvsDisinfo), there are examples of the promotion of self-interests (such as the Sputnik vaccine), generic and nation-focused content,

⁴ Cf. (Patrick D. and Gilbert, 2009).

fake news, and amplification of fake news originating from a tier and benefiting Russia. Most fuelled broader conspiracy theories⁵.

Conspiracy theories and their followers abounded during the pandemic. It can be observed that Russia contributed to their spreading, using bits of truths as Trojan horses to inoculate doubt or inaccuracies in people's minds. Disinformation (IOME1) was widely used relying on a tripod of social media (notoriously Facebook – IOME4), so-called experts like Irja Lutsar, professor of virology at the University of Tartu and head of the Scientific Advisory Board formed at the Government Committee, and vectors like *rubaltic.ru* (now banned⁶) and *Telegram.ee*⁷ (IOME2).

Individuals against masks, 5G, vaccines, or denying the pandemic formed a broader community, with an estimated 20,000 Estonians adhering to one or several theories⁸. It contributed to discontent and distrust with government policies. The tactic has been publicly acknowledged by Arnold Sinisalu, Director General of the Internal Security Service of Estonia (*Kaitsepolitseiamet*, 2023).

COVID-19 conspiracy theories in Estonia helped Russia create nodes of discontent and dissent among Estonian citizens and improved their receptivity to other narratives, such as Russia being forced into war against Ukraine as a result of NATO threats (Astapova, 2023). By fueling these theories, Russia fulfilled its operational objective of undermining Estonia's societal cohesion (OO2) while also astray a few Estonians from Western media, making them believe in other Russian-fuelled narratives (OO3).

How did the Impressum Club help to relay Russian narratives in Estonia?

To shape the information space, Russia needs not only to create disbelief through disinformation but also propose alternative narratives supporting its interests. Such narratives can be disseminated through Russian media companies abroad when they have not been banned, or resort to media friendly to Russian narratives or social

⁵ Conspiracy theories are “attempts to explain the ultimate causes of significant social and political events and circumstances with claims of secret plots by two or more powerful actors” according to Douglas et al., 2019.

⁶ Rubaltic.ru appears on the list of Foreign reprisals against Russian journalists and media since the start of the special military operation in Ukraine (as of December 12, 2023) established by the Ministry of Foreign Affairs of the Russian Federation, (Министерство иностранных дел Российской Федерации 2023b). See also (Veebel, Ploom, and Sazonov, 2022).

⁷ (Belova-Dalton, Oksona, PhD 2021).

⁸ *Ibid.*

media. However, to get a hold, an information needs validation (Boca, 1996) which can be acquired through repetition or affirmation by a rationally legitimate source (expert). Thus, Russia nurtures a network of experts complacent to its positions worldwide.

MTÜ *Impressum*, or the *Impressum* Club, was established as nonprofit organisation in October 2008 in Estonia by local entrepreneur Igor Teterin and Northern European version of the *Komosomolskaya Pravda* journalist Galina Sapozhnikova (*Kaitsepolitseiamet*, 2013). The club organised monthly talks in Tallinn's Hotel Europe. It was part of a larger international initiative in Northern and Eastern European countries, Format A3 (Latvia, Lithuania, Moldova) or Skorovoda Club (Ukraine). It is unclear whether the club still exists in Estonia. Its website is no longer accessible, and its Facebook account is not updated. Its activities were ongoing at least as far as April 2020 (Makarychev, 2021).

As demonstrated by Makarychev (*Ibid.*), this club contributed to relaying the Russian narrative in Estonia by inviting academics and experts to promote alternative positions favouring Russia's political views. According to him, out of 100 guest speakers invited, 38 had a media background, 31 were in the edition field, 23 were from the movie industry and 11 were political militants. All had some legitimacy in their field, like Peter W. Schulze, professor of political sciences, teaching at the University of Göttingen. As for the content relayed, the narratives identified by Makarychev do not differ from more recent attempts from Snigyr (2024) to build a taxonomy of strategic communication lines followed by the Kremlin and its surrogates. The conferences conveyed lines of communication to the Estonian audience. According to the Estonian Internal Security Service, this club primarily addressed the EST-RUS community.

It demonstrates the employment of IOME2 by Russia, which nurtures a web of experts ready to back its narratives. Beyond, this case presents an interest as it uncovers the conduct of what can be designated as combined information operations, where different vectors and lines of communications meet to multiply their effects in the information sphere.

How does Russia benefit from EKRE's stance?

Political parties within those organisations that are Eurosceptic or critical of the Alliance thus represent an opportunity for Russia to disseminate, relay and validate its strategic narratives. However, such parties are not necessarily aligned with Russia even though

they serve its SO. The case of EKRE is of interest. It plays for Russia when undermining the confidence of Estonians in the EU by relaying Russian strategic narratives on the decadence of the Western world and blaming the EU for the migrant crisis while brewing hatred against them (Makarychev and Sazonov, 2019). On the other hand, the hard stance of EKRE against migrants extends to Russophones whenever it reinforces their narrative, including those settled during the Soviet Occupation (*Ibid.*).

In the long run, Russian objectives collide with EKRE's views. EKRE's youth organisation former leader Ruuben Kaalep summarized this dilemma: "*In the West we have insecurity due to immigrants; in the East we have Russia which doesn't respect our independence.*" (Kaalep, 2017). Even since then EKRE seems to try to also appeal to the EST-RUS community (Lomp, 2020), its stance remains blurry and not likely to be a direct Kremlin's ally. Henceforth Russia can only partially hope EKRE to contribute to its OO, significantly influencing the Estonian audience in favour of Russian positions. However, most of its OOs are satisfied by EKRE's position and activism.

FIGHTING RUSSIAN INFORMATION OPERATIONS IN A DEMOCRATIC CONTEXT

Estonia has consistently invested in preventing disinformation with the hope that it would reduce the influence of the Russian narrative in its media space. During the COVID-19 pandemic, this strategy proved insufficient. However, Russia suffered from the ban on its state media in Estonia and the eye-opening effect the brutal aggression of Ukraine had. However, with time passing and Russia adapting its narratives, its InfoOps will likely gain momentum again. Therefore, proactive policies should be taken to address current and future campaigns against Estonia in the information space.

Media literacy – The failure of the current counterdisinformation paradigm

The European Council had acknowledged the disinformation threat as soon as 2015 when it requested the High Representative (HR) to tackle the disinformation campaigns carried out by Russia. It noticeably resulted in the creation of the EUvsDisinfo platform, which lists and answers disinformation narratives. In 2017, the Hybrid Center of Excellence was established following an EU initiative (High Representative of the European Union for Foreign Affairs and Security Policy and European Commission, 2016). Part of its mission is to monitor influence strategy and promote research, strategies, and training to circumvent influence operations. In

December 2018, the European Council endorsed an action plan. Among the principal measures was setting up a network of national contact points and a dedicated coordinating digital platform known as the Rapid Alert System (RAS). A Hybrid Fusion Cell was also created within the EEAS. The implementation of the Code of Practice on Disinformation for Online Platforms (CPD), published earlier in 2019, was to be monitored by the European Commission (EC).

Estonia has been the earliest victim of modern Russian InfoOps, as part of a broader influence campaign, which also included cyber-attack and diplomatic pressure, during the Bronze Soldier episode in 2007⁹. Following this event Estonia funded new public service television programs and online news in Russian. In 2015 it enhanced its effort through the creation of a public-funded television network (ETV+) in Russian language and the development of media literacy teachings in schools. Efforts were completed in 2016 with the Estonian Defense League (*Kaitseliit*) volunteers' initiative "Propastop", a website whose aim is to identify and debunk Russian narratives.

It should be noticed that the development of independent or state Russian-speaking media has, however, proved partly successful with rising audiences among the EST-RUS (Teperik, 2023). However, such a policy should be separate from the media literacy effort. It is instead a countermeasure to Russian InfoOps. The decision to provide some competition with media talking to EST-RUS in their language addresses the main concern on the societal cohesion of Estonian: first, the feeling of discrimination of the EST-RUS community; second, the dominance of Russian players in the media offer in their language. It directly counters Russian OO2 and 3.

The other measure that proved effective is neither preventive. The ban on prominent Russian media outlets and experts disrupted the patterns of InfoOps (IOME2). Russia felt the blow as it has carefully documented such decisions (*Министерство иностранных дел Российской Федерации*, 2023b). Among EST-RUS, this resulted in a decrease in people watching traditional media and an increase in consumption of news on social media (Teperik, 2023). Besides, antennas, dishes, Virtual Private Networks (VPNs), and extensive signals from Russia make it easy to circumvent this ban.

⁹ For a Case Study of the Bronze Soldier event, see Jankowicz, 2020.

Despite Estonian and European Union media literacy, disinformation prevention, and debunking policies, the COVID-19 period showed a sharp rise in conspiracy theories and their followers (Astapova, 2023). The effectiveness of debunking websites like Propastop, on the other hand, needs academic attention as it has yet to be assessed. In conclusion, media literacy cannot be labeled an utter failure, but its inability to prevent the dissemination of disinformation and adhesion to conspiracy theories must be acknowledged.

The effect of the Russian aggression on Ukraine on its Information Operations in Estonia

On 24th February 2022, Western Europe woke up to discover that Russia had launched a full-scale invasion of Ukraine. Actors that used to nurture ties with Kremlin-linked interests, or used to praise Russia as an alternative model, had to position themselves. In a short time, decisions like bans of television channels or expulsions of Kremlin relays, which were previously thought illiberal, were swiftly taken. Assets were frozen. Economic ties severed. As a result, traditional InfoOps relays were lost (IOME2) and political parties either praising Putin or advocating similar policies (IOME3) had to dissociate themselves from the Kremlin publicly. InfoOps were thus confined to social media (IOME4), where anonymity and lousy moderation enable trolls and disinformation to thrive.

However, no matter how eye-opening the 24th of February was across Europe, time favours Russia to reconstitute its InfoOps potential in two ways. First, the impression events make on people is volatile, and Russia has already undertaken significant efforts to camouflage aggression into a defensive operation it undertook reluctantly. Second, Russia has started taking steps to mitigate EU sanctions on its media. VPNs, satellite television, and the development of social network media are effective strategies. Speeches have also been adapted to convey the same sympathies to Russia without being censored. Talking about peace, balancing social welfare with aid to Ukraine, or blaming equally Russia and Ukraine are some of the mitigated narratives that appeared following the aggression to try and curb support for Ukraine.

Russian Information Operations are adaptative. Preventive measures have proved insufficient to curb the spreading of disinformation. Active measures taken in the aftermath of the aggression of Ukraine were but in the short term. To fight Russian

InfoOps effectively, regular, adaptative, counterdisinformation measures must be implemented.

Towards an active counterdisinformation strategy

In a democratic system, a checks and balances system safeguards citizens' liberties. Russia has been weaponizing every opportunity in democracies' legal corpus to try to influence Western voters. Public opinion is indeed a battleground. General Giap, unlike General Westmoreland, was waging war in Vietnam and in the United States, where its strategic objective was to break "America's will to fight". The inability of the Americans to see the operations in Viet Nam as only an operational level theatre, whereas the strategic battle was waged in their homeland, resulted in their defeat (Summers, 1995; Yakovleff, 2016).

The measures taken so far by Estonia have yet to prove sufficient to immunize its population from Russia. If, as said before, democracies are rooted in citizens' liberties, it is the responsibility of the state to defend them against foreign influence.

CONCLUSION

Vladimir Ilyich once said that "the Capitalists will sell us [the *Bolsheviks*] the rope with which we will hang them". Just as much as Lenin saw market-free countries as weak and hoped to take advantage of their greediness, another Vladimir seeks to choke democracies with their own freedoms.

Estonia is now a well-established and functioning democracy. The Republic has made a strong statement by joining the EU and NATO, is consistent with this decision, and is even one of the strongest advocates of both alliances. Its society supports the country's current political organisation and is culturally increasingly leaning towards the so-called Western culture.

On the other hand, Russia's imperial vision, built on layered spheres of influence, disregards sovereignty principles and the very principle of the right of peoples to self-determination. The shield of NATO has so far deterred Russia from resorting to violence to bend Estonia's will. However, Moscow is actively engaged in strategies, among which InfoOps are a tool of choice, to target the Estonian Republic's CoGs.

The case studies analysed in this article helped prove that the assumed Russian IOMEs represent patterns that can be addressed through more active countermeasures. Indeed, the preventive policies against disinformation proved insufficient to curb aggressive InfoOps. Quantitative analysis of the effectiveness of debunking hostile disinformation and the Estonian penal response to Russian InfoOps would help refine this counterdisinformation strategy.

Nevertheless, the final efficacy of the Estonian answer is linked with a broader international fight in the information space that calls for radical solutions. The regulation of the information space interests all states, and the EU could be an efficient relay of influence for Estonia to promote such a round of negotiations at the international level.

Bibliography

Academic Sources

AIDAROV, Aleksandr and DRECHSLER, Wolfgang. 2013. Estonian Russification of Non-Russian Ethnic Minorities in Estonia? A Policy Analysis. *Trames. Journal of the Humanities and Social Sciences*. 2013. Vol. 17, no. 2, p. 103. DOI 10.3176/tr.2013.2.01.

AROLD, Uku. 2016. Peculiarities of Russian Information Operations, *Sõjateadlane - Estonian Journal of Military Studies*. Vol. VI, no. 2/2016. [Online] 2021. [Cited: 10 March 2024].

https://www.ksk.edu.ee/wp-content/uploads/2016/12/sojateadlane_2_www.pdf

ASTAPOVA, Anastasiya. 2023. Conspiratorial Thinking among Russian Speakers in Estonia: From COVID-19 to the War in Ukraine. *Journal of American Folklore*. 1 October 2023. Vol. 136, no. 542, p. 361–385. DOI 10.5406/15351882.136.542.01.

AUERS, Daunis. 2018. Populism and Political Party Institutionalisation in the Three Baltic States of Estonia, Latvia and Lithuania. *Fudan Journal of the Humanities and Social Sciences*. September 2018. Vol. 11, no. 3, p. 341–355. DOI 10.1007/s40647-018-0231-1.

BELOVA-DALTON, Oksona. 2021. Spread of fake news and conspiracy theories leading to potential radicalization during COVID-19 pandemic: the case of

telegram.ee. *Proceedings*. Vol. 20th. *The Estonian Academy of Security Sciences*. [Online] 2021. [Cited: 11 September 2023]
https://digiriul.sisekaitse.ee/bitstream/handle/123456789/2840/Proceedings_2021.pdf?sequence=5&isAllowed=y

BIL, Jacek. 2022. Estonia as an Area of Russian Influence: Analysis and Synthesis of the Kremlin's Methodology of Exerting Influence on Tallinn's Political and Social Stability. *Polish Political Science Yearbook*. 2022. Vol. 51, p. 1–12. DOI 10.15804/ppsy202207.

BILBAN, Christoph and GRININGER, Hanna. 2020. Labelling Hybrid Warfare: The “Gerasimov Doctrine” in Think Tank Discourse. In: Peischel/Bilban (eds.): *Building Military Science for the Benefit of Society*. Berlin: Mises-Verlag, 2020.

BOCA, Stefano. 1996. *I processi cognitivi automatici in psicologia sociale: concettualizzazione e metodi di indagine* [Automatic cognitive processes in social psychology: conceptualisation and methods of investigation]. *Giornale Italiano di Psicologia*. 1996. Vol. 23, no. 1, p. 29–60.

BRAGHIROLI, Stefano and PETSINIS, Vassilis. 2019. Between party-systems and identity-politics: the populist and radical right in Estonia and Latvia. *European Politics and Society*. 8 August 2019. Vol. 20, no. 4, p. 431–449. DOI 10.1080/23745118.2019.1569340.

BRUBAKER, Rogers. 1996. *Nationalism reframed: nationhood and the national question in the New Europe*. Cambridge [England]; New York: Cambridge University Press. ISBN 978-0-521-57224-8.

DELONG, Marek. 2020. The Concept of Russian Federation Foreign and Security Policy by Eugene Primakov. *Internal Security*. 22 July 2020. Vol. 12, no. 1, p. 307–318. DOI 10.5604/01.3001.0014.3205.

DENISENKO, Viktor. 2022. Disinformation Analysis and Citizen Activism in the “Post-Truth” Era: The Case of DebunkEU.org. In: CHAKARS, Janis and EKMANIS, Indra (eds.), *Information Wars in the Baltic States*. [Online] 2022. Cham: Springer International Publishing. p. 169–186. The Palgrave Macmillan Series in International Political Communication. ISBN 978-3-030-99986-5.

DIGGINS, John Patrick. 1995. The Promise of Pragmatism: Modernism and the Crisis of Knowledge and Authority. University of Chicago Press. ISBN 978-0-226-14879-3.

DIKIJ, Ėvgen. 2016. The “hybrid” war of Russia: experience of Ukraine for the Baltic States. Vilnius: The General Jonas Žemaitis Military Academy of Lithuania. ISBN 978-609-8074-49-9.

DILIGENSKI, German. 2001. “The ‘West’ In Russian Public Consciousness.” *Social Sciences* Vol. 32, no. 2/2001. September 2001.

DOUGLAS, Karen M., USCINSKI, Joseph E., SUTTON, Robbie M., CICHOCKA, Aleksandra, NEFES, Turkay, ANG, Chee Siang and DERAVID, Farzin. 2019. Understanding Conspiracy Theories. *Political Psychology*. February 2019. Vol. 40, no. S1, p. 3–35. DOI 10.1111/pops.12568.

FARWELL, James P. 2020. Information warfare: forging communication strategies for twenty-first-century operational environments. Quantico, VA: Marine Corps University Press. ISBN 978-1-73200-309-5.

FREEDMAN, Lawrence and WILLIAMS, Heather. 2021. Understanding narratives and information campaigns. *Adelphi series*. 2 November 2021. Vol. 61, no. 493–495, p. 25–42. DOI 10.1080/19445571.2021.2260266.

GENTILE, Michael. 2022. How to lose the information war – Russia, fake news and the future of conflict. *Eurasian Geography and Economics*. 4 May 2022. Vol. 63, no. 3, p. 446–449. DOI 10.1080/15387216.2020.1825982.

HERB, Lin. 2020. Doctrinal Confusion and Cultural Dysfunction in DoD. *The Cyber Defense Review*. Vol. 5 n.2, no. Summer 2020, p. 89–103.

HUTCHINSON, William. 2010. Influence Operations: Action and Attitude. *Proceedings of the 11th Australian Information Warfare and Security Conference*. 2010. Edith Cowan University, p. 30. December 2010. DOI 10.4225/75/57A82E15AA0E1.

INNES, Martin, GRINNELL, Daniel, INNES, Helen, HARMSTON, Darren and ROBERTS, Colin. 2020. Normalisation et domestication de la désinformation numérique : les opérations informationnelles d’interférence et d’influence de l’extrême

droite et de l'État russe en Europe [*Normalisation and domestication of digital disinformation: the information operations of interference and influence of the extreme right and the Russian state in Europe*]. *Hérodote*. 2020. Vol. 177–178, no. 2–3, p. 101–123. DOI 10.3917/her.177.0101.

JANKOWICZ, Nina. 2020. *How to lose the information war: Russia, fake news, and the future of conflict*. London New York Oxford New Delhi Sydney: I.B. Tauris. ISBN 978-1-83860-768-5.

JUZEFOVIČS, Janis. 2022. Making Sense of Public Media in Times of Geo-Political Crisis: Latvian Public Media and their Ethno-Linguistic Majority and Minority Audiences. In: CHAKARS, Janis and EKMANIS, Indra (eds.), *Information Wars in the Baltic States*. [Online] 2022. Cham: Springer International Publishing. p. 55–79. The Palgrave Macmillan Series in International Political Communication. ISBN 978-3-030-99986-5.

KAMERĀDE, Daiga, CROTTY, Jo and LJUBOWNIKOW, Sergej. 2016. Civil liberties and Volunteering in Six Former Soviet Union Countries. *Nonprofit and Voluntary Sector Quarterly*. December 2016. Vol. 45, no. 6, p. 1150–1168. DOI 10.1177/0899764016649689.

KERSNAUSKAITE, Kristina. 2022. *Thirty Years of Democracy in Estonia and Lithuania*. Online. Harvard. Available from: <https://nrs.harvard.edu/URN-3:HUL.INSTREPOS:37373168>

KRAWCZYK, Paulina and WIŚNICKI, Jarosław. 2022. Information warfare tools and techniques in the context of information operations conducted by the Russian Federation during the 2022 war in Ukraine. *Cybersecurity and Law*. 6 December 2022. Vol. 8, no. 2, p. 278–286. DOI 10.35467/cal/157216.

KRIEG, Andreas. 2023. *Subversion: the strategic weaponization of narratives*. Washington, DC: Georgetown University Press. ISBN 978-1-64712-336-9.

LAWRENCE, Tony, 2023. Estonia: Size Matters. *PRISM*. Vol. 10, March 2023, no. 2, p. 19–37.

LOTTHOLZ, Philipp and LEMAY-HÉBERT, Nicolas. 2016. Re-reading Weber, re-conceptualizing state-building: from neo-Weberian to post-Weberian approaches to

state, legitimacy and state-building. *Cambridge Review of International Affairs*. October 2016. Vol. 29, no. 4, p. 1467–1485. DOI 10.1080/09557571.2016.1230588.

MAKARYCHEV, Andrey. 2021. Russian “cognitive propaganda”: the case of *Impressum Club* in Tallinn. *Post-Soviet Affairs*. 2 January 2021. Vol. 37, no. 1, p. 45–64. DOI 10.1080/1060586X.2020.1804259.

MAKARYCHEV, Andrey and SAZONOV, Vladimir. 2019. Populisms, popular geopolitics and the politics of belonging in Estonia. *European Politics and Society*. 18 January 2019. Vol. 20, p. 1–20. DOI 10.1080/23745118.2019.1569341.

MULLANEY, Samantha. 2023. Everything Flows. *The Cyber Defense Review*, Fall 2022, Vol. 7, No. 4, pp. 193-212.

NELSON, Taylor, KAGAN, Nicole, CRITCHLOW, Claire, HILLARD, Alan and HSU, Albert. 2020. The Danger of Misinformation in the COVID-19 Crisis. *Missouri Medicine*. 2020. Vol. 117, no. 6, p. 510–512.

NYE, Joseph S. 1990. Soft Power. *Foreign Policy*. 1990. No. 80, p. 153. DOI 10.2307/1148580.

OSKOLKOV, Petr. 2023. Estonianness in the Making: Transformations of Ethnic Democracy Model and Nationalism in Estonia. *Ethnopolitics*. 5 June 2023. P. 1–20. DOI 10.1080/17449057.2023.2216981.

PATRICK D., Allen and GILBERT, Dennis P. 2009. The Information Sphere Domain Increasing Understanding and Cooperation. 2009. Vol. *The Virtual Battlefield: Perspectives on Cyber Warfare*, no. IOS Press, p. 132–142.

PELTIER, Marie and TRIFUNOVIC, Alexandre. 2023. *Propagande et complotisme : la Russie peut-elle gagner la guerre des narratifs ?* [Propaganda and conspiracy: can Russia win the narrative war?] *Revue de la Défense Nationale*. 7 March 2023. Vol. N° 858, no. 3, p. 47–53. DOI 10.3917/rdna.858.0047.

PETERSOO, Pille. 2007. Reconsidering otherness: constructing Estonian identity. *Nations and Nationalism*. Vol. 13, no. 1, pp. 117–133. DOI <https://doi.org/10.1111/j.1469-8129.2007.00276.x>.

PLOOM, Illimar, SAZONOV, Vladimir and FOSTER, Noel. 2023. The Impact of War in Ukraine on the Political and Ideological Agenda of European Post-communist State Conservative Populists: The Case of EKRE. In: MÖLDER, Holger, VOINEA, Camelia Florela and SAZONOV, Vladimir (eds.), *Producing Cultural Change in Political Communities*. [Online] 2023. Cham: Springer Nature Switzerland. p. 217–250. Contributions to Political Science. ISBN 978-3-031-43439-6.

POLESE, Abel and SELIVERSTOVA, Oleksandra. 2020. Luxury consumption as identity markers in Tallinn: A study of Russian and Estonian everyday identity construction through consumer citizenship. *Journal of Consumer Culture*. May 2020. Vol. 20, no. 2, p. 194–215. DOI 10.1177/1469540519891276.

POLYNIN, Ivan, 2023. Patching identity. How Russian language media in Estonia reconstitutes our understanding of citizenship. *Frontiers in Political Science*. 20 April 2023. Vol. 5, p. 1140084. DOI 10.3389/fpos.2023.1140084.

PRAUSE, Gunnar, Tarmo TUISK, and Eunice Omolola OLANIYI. 2019. “Between Sustainability, Social Cohesion and Security. Regional Development in North-Eastern Estonia.” Edited by Manuela Tvaronavičienė. *Entrepreneurship and Sustainability Issues* 6, no. 3 (March 1, 2019): 1235–54. [https://doi.org/10.9770/jesi.2019.6.3\(13\)](https://doi.org/10.9770/jesi.2019.6.3(13)).

RAUDJÄRV, Matti. 2015. Economic and trade relations of Estonia as a EU member state, incl. with Russia and Ukraine. Eesti kui Euroopa Liidu liikmesriigi majandus- ja kaubandussidemed, sh Ukraina ja Venemaaga. *Estonian Discussions on Economic Policy*. [Online] 2015. Vol. 23, no. 1. DOI 10.15157/tpep.v23i1.12237.

SAZONOV, Vladimir, PLOOM, Illimar and VEEBEL, Viljar. 2022. The Kremlin’s Information Influence Campaigns in Estonia and Estonian Response in the Context of Russian-Western Relations. *TalTech Journal of European Studies*. 1 May 2022. Vol. 12, no. 1, p. 27–59. DOI 10.2478/bjes-2022-0002.

ŠEŠELGYTĖ, Margrara and BLADAITĖ, Neringa. 2021. How to Defend Society? Baltic Responses to Hybrid Threats. In: BRADY, Anne-Marie and THORHALLSSON, Baldur (eds.), *Small States and the New Security Environment*. [Online] 2021. Cham: Springer International Publishing. p. 73–86. The World of Small States. ISBN 978-3-030-51528-7.

SIMON, Felix M and CAMARGO, Chico Q. 2023. Autopsy of a metaphor: The origins, use and blind spots of the 'infodemic.' *New Media & Society*. August 2023. Vol. 25, no. 8, p. 2219–2240. DOI 10.1177/14614448211031908.

SMITH, Paul A., Jr. 1990. *On political war*. US Govt. Printing Office. ISBN 978-0-16-001719-3.

SNIGYR, Olena. 2024. Russian strategic narratives, 2022–2023. *Orbis*. 2024. Vol. 68, no. 1, p. 3–23. DOI 10.1016/j.orbis.2023.11.002.

SUMMERS, Harry G. 1995. *On strategy: a critical analysis of the Vietnam War*. Novato, CA: Presidio Press. ISBN 978-0-89141-563-3.

THEOHARY, Catherine A. 2020. Defense Primer: Information Operations. *In Focus*. 14 January 2020. Congressional Research Service.

TOOTS, Maarja. 2019. Why E-participation systems fail: The case of Estonia's Osale.ee. *Government Information Quarterly*. July 2019. Vol. 36, no. 3, p. 546–559. DOI 10.1016/j.giq.2019.02.002.

TRIFONOVA, Alina V. 2021. Role of Local Identity and Perceived Context in Psychological Well-Being of Russians in Estonia. *Cultural-Historical Psychology*. 2021. Vol. 17, no. 4, p. 83–91. DOI 10.17759/chp.2021170409.

VEEBEL, Viljar, PLOOM, Illimar and SAZONOV, Vladimir. 2022. Russian information warfare in Estonia, and Estonian countermeasures. *Lithuanian Annual Strategic Review*. 15 June 2022. Vol. 19, no. 1, p. 69–98. DOI 10.47459/lasr.2021.19.4.

VENTRE, Daniel. 2016. *Information warfare*. Revised and updated 2nd edition. London: ISTE. Information systems, web and pervasive computing series. ISBN 978-1-84821-660-0.

YAKOVLEFF, Michel. 2016. *Tactique théorique*. 3e éd. Paris: Économica. Stratégies & doctrines. ISBN 978-2-7178-6747-3.

Think Tank Sources

GALEOTTI, Mark. 2019. The Baltic States as Targets and Levers: The Role of the Region in Russian Strategy. George C. Marshall European Center For Security Studies, Security Insights, N. 027. [Online] April 2019. [Cited: 6 December 2023]. <https://www.marshallcenter.org/en/publications/security-insights/baltic-states-targets-and-levers-role-region-russian-strategy-0>

JACKSON, Jon and BATEMAN, Dean. 2024. Countering Disinformation Effectively: An Evidence-Based Policy Guide. *Carnegie Endowment for International Peace*. [Online] 2024. [Cited: 8 February 2024]. <https://carnegieendowment.org/2024/01/31/countering-disinformation-effectively-evidence-based-policy-guide-pub-91476>

JUURVEE, Ivo. 2021. The Actions of the Russian Intelligence Must Be Countered in Public. *ICDS*. Online. 27 April 2021. [Cited: 8 February 2024]. <https://icds.ee/en/the-actions-of-the-russian-intelligence-must-be-countered-in-public/>.

KALLAS, Kristina. 2021. Is Russian Minority a State Security Risk in the Baltic States? BEAR Policy Conference. [Online] May 2021. [Cited: 19 December 2023]. <http://www.bearnetwork.ca/wp-content/uploads/2021/05/Kristina-Kallas-Policy-Memo.pdf>.

MART Põrk. 2022. International Interdisciplinary Seminar on “Information Disorders in Politics, Media, and Historical Memories.” *ICDS*. [Online] 28 September 2022. [Cited: 6 December 2023]. <https://icds.ee/en/international-interdisciplinary-seminar-on-information-disorders-in-politics-media-and-historical-memories/>

PIRNIE, Bruce and GARDINER, Sam. 1996. *An objectives based approach to military campaign analysis*. Santa Monica, Calif: Rand. ISBN 978-0-8330-2397-1.

RUIZ Monica M. 2017. Impacts of Russian Information Operations: Technical and Psychological Aims. *ICDS*. [Online] 24 October 2017. [Cited: 10 March 2024]. <https://icds.ee/en/impacts-of-russian-information-operations-technical-and-psychological-aims/>.

TEPERIK, Dmitri. 2023. The Glass of Societal Resilience – Half Empty or Half Full. *ICDS*, September 2023.

TURCSÁNYI, Richard. 2023. Dragon's Roar and Bear's Howl: Convergence in Sino-Russian Information Operations in NATO Countries? NATO Strategic Communications Centre of Excellence.

Governmental Publications

COMMITTEE ON FOREIGN AFFAIRS OF THE US HOUSE OF REPRESENTATIVES, 114th CONGRESS, First Session. 2015. Serial No. 114-37- Confronting Russia's Weaponization of Information. [Online] April 15, 2015. [Cited: 7 November 2023]. <https://www.govinfo.gov/content/pkg/CHRG-114hhrg94186/html/CHRG-114hhrg94186.htm>

EUVSDISINFO. Online Database. [Cited: 8 November 2023]. <https://euvsdisinfo.eu/fr/disinformation-cases-fr/>

EUVSDISINFO. 2021. *Mise à jour du rapport spécial du SEAE: Brève évaluation des récits et éléments de désinformation circulant à propos de la pandémie de COVID-19 (mise à jour décembre 2020 – avril 2021)* [Update of the EEAS special report: Brief assessment of the stories and misinformation circulating about the COVID-19 pandemic (update December 2020 - April 2021)]. *EU vs Disinfo*. [Online] 28 April 2021. [Cited: 8 November 2023]. <https://euvsdisinfo.eu/fr/mise-a-jour-du-rapport-special-du-seae-breve-evaluation-des-recits-et-elements-de-desinformation-circulant-a-propos-de-la-pandemie-de-covid-19-mise-a-jour-decembre-2020-avril-2021/>

ESTONIAN NATIONAL ELECTORAL COMMITTEE AND THE STATE ELECTORAL OFFICE. Online Database. [Cited: 17 October 2023]. <https://www.valimised.ee/en>

GLOBAL ENGAGEMENT CENTER. 2020. *Les piliers de l'écosystème de désinformation et de propagande de la Russie [The pillars of Russia's disinformation and propaganda ecosystem]*. US Department of State, August 2020. [Online, consulted in French] January, 2022. [Cited: 11 August 2023]. <https://www.state.gov/wp-content/uploads/2022/01/LS-2020-0111499-PILLARS-OF-RUSSIA-DISINFORMATION-FRE.pdf>

KAITSEPOLITSEIAMET. 2013 – 2019 – 2020 - 2021. *Annual Reviews 2013 – 2019/2020 – 2020/2021 – 2021/2022 – 2022/2023*. Online. [Cited: 10 March 2024]. <https://kapo.ee/en/content/annual-reviews/>

KENNAN, George. 1946. “The Long Telegram”. Online. [Cited: 18 October 2023].
<https://nsarchive2.gwu.edu/coldwar/documents/episode-1/kennan.htm>

RIIGI TEATAJA. The Estonian Constitution. Online. [Cited: 4th March 2024].
<https://www.riigiteataja.ee/en/eli/530102013003/consolide>.

RIIGI TEATAJA. The Penal Code. Online. [Cited: 14 January 2024].
<https://www.riigiteataja.ee/en/eli/522012015002/consolide>

SISEMINISTEERIUM. Citizenship. Online Database. [Cited: 16 October 2023].
<https://www.siseministeerium.ee/en/activities/efficient-population-management/kodakondsus>

STATISTIKAAMET. 2022. Population census. 76% of Estonia’s population speak a foreign language, 16 November 2022. [Online]. [Cited: 17 October 2023].
<https://rahvaloendus.ee/en/news/population-census-76-estonias-population-speak-foreign-language>

THE MINISTRY OF FOREIGN AFFAIRS OF THE RUSSIAN FEDERATION. 2023. *Concept de la politique étrangère de la Fédération de Russie* [The Concept of the Foreign Policy of the Russian Federation]. [Online, consulted in French] 15 March 2023. [Cited: 30 January 2024].
https://mid.ru/en/foreign_policy/fundamental_documents/1860586/?lang=fr

THE MINISTRY OF FOREIGN AFFAIRS OF THE RUSSIAN FEDERATION. Foreign reprisals against Russian journalists and media since the start of the special military operation in Ukraine. [Online]. [Cited: 17 December 2023].
https://mid.ru/en/foreign_policy/reports/1831575/

US DEPARTMENT OF STATES, Bureau of Public Affairs. 1981. Special Report on Soviet Active Measures. U. S. Govt. Printing Office, 1981. [Online]. [Cited: 17 December 2023].
<http://insidethecoldwar.org/sites/default/files/documents/Soviet%20Active%20Measures%20Forgery,%20Disinformation,%20Political%20Operations%20October%201981.pdf>

Media Articles and other Sources

AFP. 2023. Russian minority shuns Estonia vote over Ukraine support. *France24* [Online] 5 March 2023. [Cited: 13 January 2024]. <https://www.france24.com/en/live-news/20230305-russian-minority-shuns-estonia-vote-over-ukraine-support>

HANKEWITZ, Sten. 2023. Politico: Russian paramilitary group tried to interfere with Estonian politics through EKRE. *Estonian World*. [Online] 19 February 2023. [Cited: 18 October 2023]. <https://estonianworld.com/security/politico-russian-paramilitary-group-tried-to-interfere-with-estonian-politics-through-ekre/>

KAALEP Ruuben. 2017. Our Tribal Future. [Online] published on Sinine Äratus youtube.ee account recording a conference organized by Skydas in Kaunas, Lithuania, 5 July 2017. [Cited: 12 February 2024]. <https://www.youtube.com/watch?v=cvqfof6AB-M>

KREKÓ Péter, SZICHERLE Patrik. 2020. *Läheb viiruslikuks. Covid-19 desinformatsiooni ökosüsteemis* [Going Viral – The Covid-19 Disinformation Ecosystem]. *ERR*. [Online] 23 March 2020. [Cited: 7 November 2023]. <https://kultuur.err.ee/1067673/laheb-viiruslikuks-covid-19-desinformatsiooni-okosusteemis>

LOMP, Loora-Elisabet. 2020. Interior minister to *Deutsche Welle*: Let the gays run to Sweden. *Postimees*. [Online] 19 October 2020. [Cited: 25 March 2023] <https://news.postimees.ee/7089490/interior-minister-to-deutsche-welle-let-the-gays-run-to-sweden>

PROPASTOP. 2023. Rakvere products in Russian propaganda. [Online] 25, October 2023. [Cited: 2 November 2023]. <https://www.propastop.org/eng/2023/10/25/rakvere-products-in-russian-propaganda/>

RATMAN, Anne. 2010. „Pikaajaline mälu” - raamat, mis avab silmi [Long Term Memory – An eye-opening book]. *Kesknädal*. [Online] 2010. [Cited: 20 December 2023]. https://web.archive.org/web/20160305011522/http://www.kesknadal.ee/g2/uudised?id=14070&sess_admin=272989c478b2539350007c30bd84c5fd

ROTH, Andrew. 2021. European MPs targeted by deepfake video calls imitating Russian opposition. *The Guardian*. [Online] 22 April 2021. [Cited: 6 December 2023].

<https://www.theguardian.com/world/2021/apr/22/european-mps-targeted-by-deepfake-video-calls-imitating-russian-opposition>

TURCHI, Marine. 2023. *L'argent russe du Rassemblement national* [The Russian money of the *Rassemblement National*]. *Mediapart*. [Online] 14 September 2023. [Cited: 18 October 2023].

<https://www.mediapart.fr/journal/france/dossier/largent-russe-du-rassemblement-national>

BEST ESSAY OF THE HIGHER COMMAND STUDIES COURSE (HCSC)



MAREK BIALOBRZESKI. The reason behind Russia's invasion of Ukraine?

INTRODUCTION

On February 24th, 2022, Russia's President Vladimir Putin pronounced an address to the country in which he stated a "special military operation" against Ukraine. In his official statement, he submitted the main reason to do that:

'Its goal is to protect people who have been subjected to bullying and genocide by the Kyiv regime for eight years. And for this, we will strive for the demilitarization and denazification of Ukraine, as well as bringing to justice those who committed numerous, bloody crimes against civilians, including citizens of the Russian Federation' (Putin, 2022).

This statement, which I mentioned earlier, was delivered in 2022 when the Kremlin started a full-scale invasion, the second part of Russia's brutal attack on Ukraine. The very beginning, however, commenced in 2013 when massive protests appeared in Ukraine when pro-Russia contemporary President Viktor Yanukovich made a decision to abandon the European Union (EU) association deal. Fortunately, this unfavourable situation in Ukraine did not take long. The significant turning point for Ukraine was in 2014 when President Yanukovich was forced to dethrone from his position and flee the country. Since then, Ukraine's situation has steadily grown to regain close relations with the EU.

That is why, in the same month, Putin decided to seize southern and eastern parts of Ukraine, the country that gained its independence thirteen years earlier after the Soviet Union collapsed. Firstly, the Crimea Peninsula was utilized by the so-called 'little green man.' Still, they were Russian soldiers without insignia or any other identification not to be identified. Next, eastern parts of the Luhansk and Donetsk areas were taken by pro-Russian separatists.

In this Research Paper, I will explain why Putin's official statement to invade Ukraine was only a mythical reason to justify Russia's invasion. Thus, it is essential to present a genuine reason for what precisely drove Putin to invade Ukraine. Many articles

concerning this topic have been published in which we can find a lot of reliable reasons to understand Putin's decision. Most well-known military analysts or journalists who tried to discover the real reason behind Russia's invasion of Ukraine agree that within those reasons, there are some with the highest importance. Among them, we can find ethnic, historical, and imperial reasons, Putin's regime ideology, domestic issues, or geopolitical reasons. Therefore, this paper will focus on the geopolitical reasons, which, in my opinion, was the veritable purpose that pushed Putin to invade Ukraine.

It is essential for the North Atlantic Treaty Organization (NATO), especially for the NATO eastern flank countries, to realize what motivates the Russian president's decision-making process. Understanding Putin's behaviour, Kremlin's strategy thinking, and international relations between Russia and the West is crucial. Understanding this challenging issue can provide Western countries with priceless information, such as proper deterrence posture or preparation for modern and future threats.

This work will provide a solid foundation for my thesis statement. The first chapter will focus on geopolitical backgrounds and offer basic information on two geopolitical components - security concerns and strategic control. I consider those two factors facilitative, which is why they will be described in the first section. The second chapter will focus on great power and regional domination to present logic, evidence, and observations for this reason. In conclusion, I will summarize the findings and provide recommendations for the future.

SECURITY CONCERNS AND STRATEGIC CONTROL

Geopolitical reasons that pushed President Putin to decide to invade Ukraine are many-faced and layered, stricken by many factors such as security concerns, strategic control, regaining regional domination, and rebuilding Great Power status. Russia's elites believe that NATO enlargement breached their businesses and interests and violated Russia's space security. According to Moscow's elites, to rebuild Russia's great power status, Ukraine must be in its sphere of influence (Tsyganov, 2008).

Russia's President Vladimir Putin, in his speech in February 2022, introduced his point of view on his country's concerns. In his statement, he said that NATO enlargement is

a fundamental threat, which, year by year, step by step, roughly and unceremoniously, is drawn by irresponsible Western politicians against Russia. In his opinion, NATO's enlargement in the east direction and its nearing military infrastructure at Russia's border are unacceptable (Putin, 2022).

Elias Götz and Jørgen Staun believe that vulnerability to external attack is a part of Russia's strategic culture (Götz, Staun, 2022). Because Russia possesses vast territory and long frontiers, it is hard to protect all of Russia's land from many directions simultaneously. Looking deep into history, we can easily find paradigms in which Russia was often invaded in the last centuries. In the thirteenth century, Mongol leader Genghis Khan and later his successors invaded, conquered, and ruled parts of Russia's lands for several centuries. Afterward, French Emperor Napoleon Bonaparte invaded Russia in the nineteenth century, and eventually, during the First and Second World Wars, Russia was attacked by various foreign countries. This historical recollection is deeply rooted in Russia's strategic thought. That is why Russia's war analytics, elites, and leadership took into mind the fact that their country must control its neighbourhood and that Russia must own a buffer zone to head the enemy off. For Russia, possessing its strategic depth is the highest priority purpose. Fyodor Lukyanov, Editor in Chief of Russia in Global Affairs and Chairman of the Presidium of the Council on Foreign and Defense Policy abstracts this narrative: 'As a country of plains,' he writes, 'Russia has experienced devastating invasions more than once; the Kremlin has long seen reinforcing 'strategic depth' as the only way to guarantee its survival' (Lukyanov, 2016).

Another aspect of vulnerability and fear, presented by Götz and Staun, concerns Russia's entrenched constant fear of thwarting NATO. This fear originated from the previous wars that Russia fought with the West. Ukraine's and Belarus's plain terrains conceive convenient conditions for aggressors to conduct attacks on Russia's soil. After World War II, the situation remained almost the same. During the Cold War, the Soviet Union felt constant stress from NATO, especially the United States. Thus, it is clear that Putin's inner circle advisers perceive Ukraine's pro-western posture as a potential threat of the highest importance. Götz and Staun cover the latest changes in Russia's official military documents. In 1993, National Security Strategies and Russian Military Doctrines claimed that NATO enlargement was one of the most problematic threats (Bakshi, 2000). The situation became even more severe in 2014

and 2021 when Russian officials got a new Military Doctrine into print (Russian et al., 2020). In this document, it was written that NATO enlargement and the new alliance's military compounds in close vicinity of Russia's borders were among the main risks.

Putin, during his work as a KGB agent in the late 1980s in Dresden, Germany, witnessed the Berlin Wall collapse, the demise of the communist regimes, and the rise of pro-democratic values. This situation made him aware that authoritarian regimes are vulnerable, especially when the authoritarian country borders a democratic state. This event showed him the power of people and the power of the public-spirit movement to effect change. Revolution in Eastern Europe gave him a sense of fear and anxiety that this system could also appear in the Soviet Union. This kind of fear, the threat that Ukraine, as a post-soviet country, could transform into a West-oriented one, Götz and Staun also put into consideration in their article. They present this threat as a combination of internal and external factors, a cyclical subject of Soviet military scripts. This concern circled back to Russian strategic thinking after the so-called 'colour revolution.' The first one appeared in Georgia in 2003 and was named the 'Rose Revolution'; the following year, in Ukraine, it was named 'Orange Revolution,' and eventually the 'Tulip Revolution' in Kyrgyzstan in 2005. This threat is magnified because Russia's leadership thought that the West wanted not only to change the regime in Moscow but also in the rest of the post-Soviet countries. They believed the West wished to upset Russia's sphere of influence and to change Russia's Commonwealth of Independent States (CIS). The former Federal Security Service of the Russian Federation (FSB) Chief Nikolai Patrushev, in 2005, said: 'Our opponents purposefully and consistently seek to weaken Russian influence in the CIS space (...). Recent events in Georgia, Ukraine, and Kyrgyzstan confirm this' (Patrushev, 2005). Also, Valery Gerasimov, former Russian Chief of General Staff, in 2013 suggested that the 'colour revolutions' were organized by external actors led by the West (Gerasimov, 2013). This thinking was transformed into the official latest Russian documents, such as foreign policies, doctrines, or strategies.

Kremlin strongly believed that Ukraine, a post-soviet country, could not be transformed into a democratic nation because it would directly threaten democratic diffusion on Russia's soil. It was unacceptable that a state neighboring Russia could integrate with the West. Moscow strongly believed that NATO provoked Russia and that Putin was put against the wall. That is why a pre-emptive strike was a defensive act against the

West. In February 2022, Russia's Foreign Policy analyst Dmitri Trenin told the press that:

'No degree of NATO expansion, including to incorporate Ukraine, will threaten the military balance and deterrence stability...Therefore, in terms of military security, it's correct to say I don't see NATO expansion as such a terrible threat...But there is another factor: a country that becomes a NATO member undergoes profound reformatting, which touches upon all walks of life. The country transforms politically and ideologically. While Ukraine is outside of NATO, it's still possible that the entire country or some part of it may decide that the Slavic identity, the 'Russian world,' and other things matter, and this may lead to a normalization of relations with Russia, and even closer relations with it. At least, from Moscow's vantage point, such a possibility remains. But if a country joins NATO, that's it: that ship has sailed. In this sense, yes, there is a threat but not a military one; rather, it's geopolitical and geocultural' (Trenin, 2022).

Another geopolitical factor that pushed Russia to invade Ukraine was strategic control. According to Jokull Johannesson and David Clowes: 'Russian control of both Ukraine's energy markets and resources for its use and their strategic denial to the EU was the key motive for Russia's aggression towards Ukraine' (Johannesson, Clowes, 2020). In March 2014, President Putin, in his appeal to the Federation Council, said that Russia's military forces based in the Crimea Peninsula were under high threat at that time (Putin, 2014). Defense Minister Sergei Shoigu presented the same rhetoric. He warned that Russian military infrastructure could be taken over, which is why some steps must be taken to tighten security in this area (Allison, 2014). This narrative was, of course, the only official reason for Putin to seize Crimea, but not so far as a true one. Roy Allison describes that the decision to invade Ukraine was made in 2008 because of the chance of Ukraine becoming a NATO member shortly (Allison, 2014). Russia planned to affiliate Ukraine with the Collective Security Treaty Organisation (CSTO) to maintain a geopolitical buffer zone between NATO and Russia. Former Russian President Dmitry Medvedev, in May 2010, said: 'Life does change, and if Ukraine decides to join the CSTO in the future, we would be happy to open the door for you and welcome you into our ranks' (Speech and discussion, 2010). According to Allison, a buffer zone could work as a security means and economically. At that time, Moscow was eager to join Ukraine in its Eurasian Economic Union built on the customs union. If so, this safety area would also be between Russia and the EU. According to former Putin's senior

adviser Sergei Glazyev, Ukraine's will to affiliate with UE instead of the customs union was unaccountable and unacceptable to Russia, and that would mean that Ukraine would no longer be a strategic partner (Glazyev, 2013). In March 2014, Putin, in response to Kyiv's declaration on NATO joining willingness, said that it: 'would have meant that NATO's navy would be right there in this city of Russia's military glory, creating a perfectly real threat to the whole of southern Russia.' In April, he declared that if the NATO soldiers were based in Crimea, 'Russia would be practically ousted from the Black Sea area. We would be left with just a small coastline of 450 or 600km' (Interview with Glazyev, 2013). Eventually, in June, he pointed out that 'we could not allow a historical part of the Russian territory with a predominantly ethnic Russian population to be incorporated into an international military alliance ... NATO infrastructure ... directly towards the Russian border' (Putin, 2014).

The possibility of putting Ukraine in Russia's international structure, the belief that Ukraine must be a part of Russia's natural sphere of influence, and the Crimea annexation, which meant denying NATO and EU members for Ukraine and maintaining military advantage in the Black Sea region, were strategic factors that influenced Putin's decision.

REBUILDING GREAT POWER STATUS AND REGIONAL DOMINATION

The previous chapter explained the geopolitical reasons why Putin invaded Ukraine in two strands – security concerns and strategic control. However, I mentioned in the introduction that these two factors were only facilitative. In this section, I will analyze geopolitical reasons in two different areas – great power status and regional domination, which, in my opinion, were more reliable when the decision to invade Ukraine was made.

To fully understand why it is so crucial for the Russian president to rebuild his country's great power status, Putin's television speech from 2005 must be cited: 'First and foremost, it is worth acknowledging that the demise of the Soviet Union was the greatest geopolitical catastrophe of the century ... As for the Russian people, it became a genuine tragedy. Tens of millions of our fellow citizens and countrymen found themselves beyond the fringes of Russian territory. The epidemic of collapse has spilled over to Russia itself' (Putin, 2005).

Tom Casier claimed that after the Soviet Union collapsed, the Russian elite's idea to rebuild their country's previous structure was the primary objective within the official discussion on the future of Russia (Casier, 2023). The Kremlin did not allow thoughts to enter their mind that Russia was no longer a great power, an Empire. Moscow's leader's imperial mindset did not disappear after 1991, as did the colonial past. In the past, Russia was an empire that successively conquered its neighboring countries, captured their population, and implemented *russskiy mir* (Russian world) (Polegkyi, Bushuyev, 2022). Due to the speed of this colonial conquest, Russia did not have time to establish its transparent concept of nation. Part of the conquered land stayed with their identities when the rest were Russified. Also, borders among those lands, among the center and periphery, the colonies, and the fatherland were blurred. Thus, when the Soviet Union collapsed and Russia suddenly found itself within restricted borders, it sustained a complicated national relationship with its national identity. Casier depicted that Russia suffered from 'national loneliness,' so elites started to think about reuniting former Soviet Union countries, especially Belarus and Ukraine, and bringing them back to Moscow's natural sphere of influence. In July 2021, Russia's President Vladimir Putin released an essay, 'On the Historical Unity of Russians and Ukrainians,' in which he claimed that Russia, Ukraine, and Belarus are one people:

'I am confident that true sovereignty of Ukraine is possible only in partnership with Russia. Our spiritual, human, and civilizational ties formed for centuries and have their origins in the same sources. They have been hardened by common trials, achievements, and victories. Our kinship has been transmitted from generation to generation. It is in the hearts and the memory of people living in modern Russia and Ukraine, in the blood ties that unite millions of our families. We have always been and will many times be stronger and more successful, for we are one people' (Putin, 2021).

Next year, in February 2022, directly before the 'special military operation,' Putin continued his thoughts. He said: 'Modern Ukraine was entirely created by Russia or, to be more precise, by Bolshevik, Communist Russia' and 'never had stable traditions of real statehood' (Putin, 2022). In his way of thinking, Ukraine was an inherent element of Russia's history, spiritual space, and culture, which is why the Kremlin had the power to take it over. According to Casier, this attitude does not present Russia as an empire that expands its territories but as an empire eligible to control lands that previously belonged to Russia. That is why the Kremlin perceives itself not as a colonial empire but, as a matter of fact, an anti-colonial country. A country that protects the other

weaker states from the colonial will of the West. After the annexation of the eastern regions of Ukraine in September 2022, Putin said: 'Deep down, the Western elites have remained the same colonizers. They discriminate and divide people into the top tier and the rest...While we – we are proud that in the 20th century, our country led the anti-colonial movement' (Putin, 2023). This statement aimed to justify Russia's imperialistic will to expand its territory and to hide its genuine reason. Casier explained later that Russia's will to expand its borders is closely related to the traditional concept of *derzhavnost* (greatpowerness). In compliance with that concept, Moscow has prestige, strength, dignity, and a right to assert power and influence beyond its borders in the global arena. This posture was often presented in Russia's foreign policies after the Soviet Union collapsed, in most cases as a concept of *russskiy mir* (Polegkyi, Bushuyev, 2022). The article's author states: 'In the mindset of the Kremlin, Russia could only be great Russia if it constituted a greater Russia' (Casier, 2023). That means that Russia's bred-in-the-bone way of thinking blends territorial expansion with a great power status.

Taras Kuzio's article "Why Russia invaded Ukraine" presents a similar way of thinking (Kuzio, 2022). He explains that Putin decided to attack Ukraine because he is obsessed with Ukraine. He believes that Ukraine, the so-called Little Russia, Belarus's so-called White Russia, and Russia as a Great Russia are part of the pan-Russian nation. It showed that Putin adopted Tsarist Russian imperial nationalism, the idea of gathering the Russian Lands, and Kyivan Rus reconstitution. This means that since these three East Slavs were born in Kyivan Rus, they are an indissoluble part of a pan-Russian nation. Putin's conspiratorial mindset assumes that Ukraine is an artificial country built firstly by Austrians, Poles, and Lenin in previous centuries and by the US and EU in recent ones. He claims that Ukraine is a puppet state led by the US, a country that is trying not to allow Ukraine to fulfill its destination and become part of Russia. Putin has an intense nostalgia for Soviet times and for a contemporary regime, which is why he is so obsessed and reluctant to identify Ukraine as a sovereign country. The Kremlin considers Ukraine to belong to *russskiy mir* - the core of the Eurasian Economic Union, where the Kremlin acts as a leader and older brother. According to Kuzio, Russia's leader is a sociopath, living in a parallel universe with no scruples for Ukrainians, feeling an enormous desire to revenge the West for lack of respect for Great Russia.

Elias Götz and Jørgen Staun present similar evidence contributing to Russia's willingness to regain its regional domination and rebuild its great power status. They cite many speeches that Putin and his inner circle addressed concerning this issue. Additionally, this narrative was also included in Russian strategy documents in which Kremlin elites presented evolvement of regional 'great power' (*veliko derzhav*) to 'leading world powers' (*lidoruyushchikh mirovykh derzhav*) (Götz, Staun, 2022). This way of thinking can be seen in previous speeches by Tsarist, Soviet, and Russian leaders, such as former President Yeltsin. Authors describe Moscow's political elites' mentality as recognizing that Russia was created to be a great power that reached several decades if not centuries. It is an existential matter, and without great power status, it will not be able to exist.

Sergey Lavrov, Russia's Foreign Minister, introduced this thinking in one of his speeches in 2007: 'Russia can (...) only exist within its present borders if it is one of the world's leading states' (Tsygankov, 2008). Elias and Staun emphasize the importance of Russia's great power desire, closely associated with its willingness to possess its sphere of influence. Moscow believed that international politics should be based on the system in which countries with great power status must own their geographical sphere of influence. Moreover, the Kremlin strongly believed that indisputable sovereignty could be related only to great power and that smaller countries' sovereignty is relevant and negotiable. Thus, the Kremlin needed to rebuild its geopolitical power and maintain regional domination. To support that opinion, former Russian President Yeltsin's decree concerning the strategic course of Russia with the member states of the Commonwealth of Independent States was presented. In this decree, Yeltsin stated that the Kremlin's willingness to create a 'leading position' allowed Russia to 'claim a worthy place in the world community' (Götz, Staun, 2022). After that, the authors give us an example of continuing this posture by presenting Putin's plan to create the Eurasian Economic Union. The primary purpose of this customs union was to reintegrate all post-Soviet states into one organism, with Moscow as the leader, and with the prospect of becoming 'one of the poles in a future multipolar world' (Götz, Staun, 2022).

According to the Kremlin, Ukraine lies in the centre of gravity of its sphere of influence. Russia could not be a great power again without this most pivotal, prominent, and significant country. In 1996, Sergey Kortunov, the former Russian president's adviser,

said: 'The direction of priority in Russia's policy in the CIS are relations with Ukraine. In perspective, our relations must acquire an allied character ... Without a strategic alliance with Ukraine, Russia will not become a genuinely great power' (Kortunov, 1996). In 2013, Anatoly Lukyanov, a former Russian Communist politician, presented an opinion: 'The (Eurasian Union] project is in fact not focused on Eurasia as a whole but on one particular country that is actually located in Europe – Ukraine. (...) If Ukraine, with its large market and potential for a strong and diversified economy, joins, it could become a major force to be reckoned with' (Lukyanov, 2013). The most transparent example of Ukraine and other post-Soviet countries' importance in Russia's point of view was presented by Moscow in December 2021 in a statement addressed to NATO and the US especially. It requested the Kremlin demand for an official declaration that Ukraine and the rest of the post-Soviet countries would never be a part of NATO. Moreover, Russia claimed the withdrawal of all US troops from contemporary NATO east flank countries. This demand meant that the West must recognize Russia's sphere of influence (The Guardians, 2021).

Zbigniew Brzezinski, a Polish American diplomat and political scientist, introduced similar statements (Brzezinski, 1997). In 1997, in his book concerning American primacy and geostrategic imperatives, he depicts that among post-soviet states, there were three of them with the highest importance: Azerbaijan, Uzbekistan, and the most important one - Ukraine. According to Brzezinski:

'Without Ukraine, Russia ceases to be a Eurasian empire. Russia without Ukraine can still strive for imperial status, but it would then become a predominantly Asian imperial state, more likely to be drawn into debilitating conflicts with aroused Central Asians, who would then be resentful of the loss of their recent independence and would be supported by their fellow Islamic states to the south.'

Furthermore, he claimed that if Russia takes control over Ukraine, a country rich in people and significant resources, and what is most crucial, the possibility of free movement within the Black Sea, it could become a great power again.

CONCLUSION

This paper analyzed my thesis statement's correctness and presented what was the genuine reason why Putin decided to invade Ukraine. It proved that Putin's official statement to invade Ukraine was the only mythical reason to justify Russia's invasion

and that the veritable purpose behind the attack was geopolitics. Firstly, I presented two facilitative pillars of geopolitical reason: security concerns and strategic control. Next, my work focused on great power and regional domination.

The first chapter paid attention to Russia's security concerns and strategic control. In this chapter, I evidenced that NATO enlargement was a fundamental threat that violated Russia's space security. Then, I showed that Russia's feeling of vulnerability came from its lessons from history, from devastating invasions from the West. This is why Russia believed it must possess a strategic depth, a buffer zone in the form of Ukraine. Next, it was presented that Moscow was concerned with the processes being implemented in Ukraine to become a pro-western country with a democratic regime. That trajectory could be 'contagious' for Russia, directly threatening democratic diffusion on Russia's soil. That is why Moscow strongly believed that Russia was 'forced' to conduct a pre-emptive strike as a defense act by the West. Finally, in this chapter, I introduced Ukraine's importance in Moscow's eyes regarding strategic control.

In the second chapter, I gathered observations and evidence concerning the rebuilding of great power status and regional domination. Firstly, I showed that for Putin, the collapse of the Soviet Union was the greatest geopolitical catastrophe of the century and that it was the most crucial objective for Russia to rebuild it (Putin, 2005). I connected Russia's will to be a great power with the Kremlin's imperial mindset. Moreover, it was said that Putin strongly believed that Ukraine and Russia are one nation and that only close cooperation with Russia could allow Ukraine to be a sovereign state. What is more, I evidenced that Putin trusted that Ukraine is an artificial country, a puppet state led by the US. Next, it was depicted that Moscow trusted that it must reshape its geographical sphere of influence to maintain its regional domination and rebuild its great power status. Thus, since Ukraine lies in Russia's centre of gravity, the Kremlin had the power to take it over.

To conclude my paper, I would like to present why it is essential to understand Moscow's way of thinking and Russia's attitude toward the West. As I have evidenced in previous chapters, the Kremlin's strategic goal for the future is to rebuild its sphere of influence and take control over post-Soviet countries to maintain a great power status. As Taras Kuzio summed up his article: 'Putin is obsessed, paranoid, angry, and

bitter. His 22 years in power have revealed him to be a sociopath with no feeling for the loss of Russian or non-Russian lives' (Polegkyi, Bushuyev, 2022). It means that Putin and all of Russia's elites are unlikely to back down and will do everything that they can to reach that objective, no matter how costly it will be. Besides, Russian society is used to shortcomings and is prepared to tolerate repression to feel security and stability. Considering the high level of security apparatus, tightened censorship, and appropriate propaganda, the advocacy among Russia's society will probably only grow or at least stay at the same level. That unfavourable situation for Ukraine and other post-soviet states would finally only encourage Moscow in their belief. Considering that Putin could stay in power till 2036, it is implausible that such a situation may change.

Fortunately, Putin's assumptions were wrong. He thought that Ukraine could be easily conquered within a few days and that the new pro-Russian government would be established. In Moscow's eyes, such a situation could enable Russia to reconfigure the new European order and break up the current American system. Thankfully, Putin did not consider that Ukraine was well prepared, that Ukraine's Army learned its lessons from 2014, and that President Zelensky emerged as a brave and firm leader. Moscow considered NATO a weak treaty organization that could not be able to act fast, effectively, and unanimously. The Kremlin outbid Russia's objectives. Nowadays, NATO is stronger than ever, more coherent, and reinforced by two new sturdy members. After Finland acceded to NATO, the alliance's border with Russia stretched more than twice. Military spending in NATO countries reached a level unseen in all treaty history, and assumptions to increase it are highly likely in the next few years. Thanks to that, Ukraine has courageously fought and resisted a brutal enemy for over two years. However, more decisions must be made to stop the enemy's advance and regain Ukraine's territories.

Thus, efforts are needed to develop suitable solutions and determine how to act and prepare for future threats from Russia. Since dialog between Moscow and the West seems unlikely, we must do our best to support Ukraine. In order to achieve that goal, the decision to increase the level of assistance must be made. NATO, and especially eastern flank countries, should rethink their current strategy. Such ideas as intelligence sharing enhancement among NATO countries, military posture, cyber defense, and hybrid threat response should be re-considered. Consolidating cohesion within NATO

and EU members or changing deterrence from punishment into deterrence by denial could also be another recommendation.

Bibliography

Allison, Roy. 2014. “Russian ‘deniable’ intervention in Ukraine: how and why Russia broke the rules.” *International Affairs* 90: 6, 2014.

Bakshi, Jyotsna. 2000. Russia's National Security Concepts and Military Doctrines: Continuity and Change. October 2000.

Russia's National Security Concepts and Military Doctrines: Continuity and Change (columbia.edu).

Brzezinski, Zbigniew. 1997. “The grand chessboard. American Primacy and Its Geostrategic Imperatives”. 1997.

https://www.cia.gov/library/abbottabad-compound/BD/BD4CE651B07CCB8CB069F9999F0EADDEE_Zbigniew_Brzezinski_-_The_Grand_ChessBoard.pdf.

Casier, Tom. 2023. No Great Russia without Greater Russia: The Kremlin’s Thinking behind the Invasion of Ukraine. *Canadian Journal of European and Russian Studies*, 16 (2)2023.

Gerasimov, Valery. 2013. Cennost’ nauki v predvidenii [The value of science is in the foresight]. *Military-Industrial Kurier*. 2013.

<https://vpk-news.ru/articles/14632>

Glazyev, Sergei. 2013. Interview with Sergei Glazyev, an adviser to Putin on regional trade, on Rossiya 24 TV channel, 27 Aug. 2013.

<http://www.russialist.org/archives/index-archive.php>, accessed 30 Aug. 2013.

Götz Elias, Staun Jørgen. 2022. “Why Russia attacked Ukraine: Strategic culture and radicalized narratives.” 01 June 2022.

Johannesson Jokull, David Clowes. 2020. “Energy Resources and Markets – Perspectives on the Russia–Ukraine War.” *European Review* 30 (1): 4-23. 06 July 2020.

<https://www.cambridge.org/core/journals/european-review/article/abs/energy-resources-and-markets-perspectives-on-the-russiaukraine-war/73B961F7835CCF710E84287BD43E9381#>.

Kuzio, Taras. 2022. “Why Russia invaded Ukraine”. Horizons. Summer 2022, No.21.

Kortunov, Sergey. 1996. “Russia in search of allies. International Affairs” (Moscow), 42(3), 148–163.

Lukyanov, Fyodor. 2016. Putin’s foreign policy: The quest to restore Russia’s rightful place. Foreign Affairs, 95(3), 30–37.

<http://www.jstor.org/stable/43946855>.

Lukyanov, Fyodor. 2013. “Russia and Ukraine on the verge of a decisive choice”. RIA-Novosti. 22 August 2013.

<https://russialist.org/russia-and-ukraine-on-the-verge-of-a-decisivechoice/>.

Polegkyi Oleksii, Bushuyev Dmytro. 2022. Russian foreign policy and the origins of the “Russian World”. 6 September 2022.

Russian foreign policy and the origins of the “Russian World” - Forum for Ukrainian Studies (ukrainian-studies.ca).

Patrushev, Nikolai. 2005. Speech at State Duma Plenary Session. 5 December 2005.

<http://transcript.duma.gov.ru/node/1089/#sel>.

Putin, Vladimir. 2022. Vladimir Putin's Speech on Ukraine, and Recognition of Donbass. (Online) 21 February 2022.

<https://www.youtube.com/watch?v=X5-ZdTGLmZo>.

Putin, Vladimir. 2014. ‘Vladimir Putin submitted appeal to the Federation Council’, 1 March 2014.

<http://eng.kremlin.ru/news/6751>.

Putin, Vladimir. 2014. Address by Putin, 18 March 2014; Direct Line interview with Putin, 17 April 2014; Putin’s interview with Radio Europe 1 and TF1 TV channel, 4 June 2014.

Putin, Vladimir. 2005. Putin: “collapse of the Soviet Union was a major geopolitical disaster of the century”. (Online) April 2005.

Putin: "collapse of the Soviet Union was a major geopolitical disaster of the century" (Eng 2005) (youtube.com).

Putin, Vladimir. 2021. Article by Vladimir Putin “On the Historical Unity of Russians and Ukrainians.” President of Russia. 2021.

<http://en.kremlin.ru/events/president/news/66181>

Putin, Vladimir. 2022. “Address by the President of the Russian Federation.” 21 February 2022.

<http://en.kremlin.ru/events/president/news/67828>.

Putin, Vladimir. 2023. “Signing of Treaties on Accession of Donetsk and Lugansk People’s Republics and Zaporozhye and Kherson Regions to Russia.”.10 February 2023.

<http://en.kremlin.ru/events/president/news/69465>.

Russian Armed Forces. 2020. Military Doctrine and Strategy. 20 August 2020.

[Russian Armed Forces: Military Doctrine and Strategy \(fas.org\)](https://fas.org/irp/publications/russian-military-doctrine-and-strategy/)

Cooper, Julian. 2021. Russia’s updated National Security Strategy, 19 July 2021.

[NDC - Research \(nato.int\)](https://www.nato.int/docu/Security/2021/210719russia.htm)

Speech and discussion. 2010. Speech and discussion with students in Kyiv. 18 May 2010.

<http://eng.kremlin.ru/news/202>.

The Guardians. 2021. “Russia issues list of demands it says must be met to lower tensions in Europe.” 17 December 2021.

<https://www.theguardian.com/world/2021/dec/17/russia-issues-list-demands-tensions-europe-ukraine-nato>.

Trenin, Dmitri. 2022. “Are We on the Brink of War? An Interview with Dmitri Trenin.” Carnegie Endowment for International Peace. 29 January 2022. Accessed 10 February 2023.

<https://carnegiemoscow.org/commentary/86304>.

Tsygankov, Aleksander. 2008. Russia’s international assertiveness. What does it mean for the West? Problems of Post-Communism, 55(2), 38–55.

<https://doi.org/10.2753/PPC1075-8216550204>.

COL MIROSLAV BORSUK. Technological Evolution and the Perception of Hybrid Warfare in Contemporary Conflicts

Introduction

‘To subdue the enemy without fighting
is the acme of skill.’

(Sun Tzu, 1963, p.73)

These quotes from the ancient military strategist Sun Tzu describe the fundamentals of hybrid warfare, which are ultimate and most convenient for every actor in the modern world. The expansion of the technology and digital sector at the beginning of the 21st century brought unconventional hybrid tactics, which became increasingly relevant with their reach, importance, and cost-effectiveness. Significant technological advances and emerging artificial intelligence (AI) have substantially developed hybrid capabilities. Russia's invasion of Ukraine in 2014 brought a significant return to the theme of hybrid operations not only in the military but also in diplomacy, business, and the media. In response to the Arab Spring, ‘General Gerasimov said: ‘The rules of war have changed. The role of non-military means of achieving political and strategic goals has grown, and in many cases, they have exceeded the power of force of weapons in their effectiveness.’ (Gerasimov, 2016, p.24).

Thus, the question remains: To what extent has rapid technological progress and the massive integration of AI into HW changed warfare? The world has witnessed many hybrid activities over the past few decades, and security experts, analysts, and scientists have studied them. The results of these scientific studies have confirmed a lack of a general definition and clear conceptual clarity of HW. Most significant is the deficit in the definition of legality and the necessity of law. There is also confusion in HW about the line between peace and war. (Bilal, 2021).

This paper, therefore, argues that digital and technological progress is changing the HW landscape, expanding the grey zone and reshaping the perception of war and peace. To clarify this claim, the individual sections of the research discuss the implications of technological developments and innovations examined at the HW. The study will focus on the new unconventional aspects of HW and shed light on the emerging AI and cognitive domain. The research paper explains how technological evolution enabled new threats and attacks. Further, how it shapes the perception of HW and the nature of the Grey Zone (GZ). Additionally, it examines whether technological advances contribute to a new type of warfare or merely modify the old concept of warfare and its perception. The remainder of this paper summarises the paragraphs and highlights the challenges for the future. This article aims to understand better the implications and connections between technological development and the nature of non-kinetic HW. Therefore, understanding innovative technologies' complexity and impact on HW helps assess risks and identify adaptive responses and proactive measures.

1. Technological Evolution and Non-Kinetic Hybrid Warfare

2.

Advanced technologies represent a radical change in the modern era of humanity that shapes our lives. The 2021 NATO Summit Communiqué in Brussels states: 'The speed of technological change has never been higher, creating both new opportunities and risks in the security environment and to the way NATO operates. We are determined to preserve our technological edge and ensure Alliance interoperability to maintain the credibility of our deterrence and defence posture.' (NATO, 2021). This describes the significant importance of technical progress for NATO. With the gradual development of communication technologies and the Internet, technical solutions appeared on the market that enabled genuinely global reach. Technology and social media are blurring the lines between an impersonal environment and an individual's identity, and maintaining social connections is critical in today's world. There are no geographical barriers to communication, and people interact online. The latest technological advancement is AI, a powerful and intelligent digital tool that can learn and think like humans. Generative AI makes breakthroughs by blurring the boundaries between human and machine creativity. AI is undoubtedly the way of the future, and its capabilities are increasingly approaching those of a human (Lamey, 2023).

The expansion of digital and information technologies to a wide range of users enabled new concepts of information warfare (IW), using AI and cyber warfare (CW) as a dominant, fundamental, and integral part of HW. These non-kinetic forms are components of current HW, often described as the fifth generation of warfare. Daniel Abbott describes it as a war of information and perception (Abbott, 2010). According to another researcher, non-kinetic or irregular warfare is network-centric, creating community tensions and facilitating a move away from state-centric nationalism (Patel, 2021). Recently, American scientist Krishnan claimed that HW expands the battlespace beyond fourth-generation warfare into political and cognitive domains. Although combat-like activities can occur in any domain, human terrain and perception are the key battlegrounds (Krishnan, 2022). German scientists see technological development as a platform for expanding hybrid threads, whose disruptive power will also bring new forms of violence. He also argues that the capabilities and capacities of modern technologies are poorly understood and that military and civilian officials need to be more aware of their disruptive nature (Thiele, et al., 2020).

Effective use of HW tools is undoubtedly possible due to rapid technological development. This would not be the case without them, and their effectiveness would be significantly reduced. Military scientists and thinkers agree that the advancement of modern technologies and the emergence of social and digital media have led to new methods, options and applications for hybrid elements of warfare. IW was widely used in recent decades, but AI as a new phenomenon has revolutionised the role of non-kinetic forms of HW, raising questions about the scale and scope of their impact on various aspects of our lives. (Gerasimov, 2016), (Weissmann, 2019), (Thiele, 2021), (Krishnan, 2022). They identify three common elements of HW that have been changed or shaped by technological development. These essential elements are:

The ways and means have changed.

The battlefield has changed.

The hybrid activities move to the new domain.

2. New Tech-driven Info and Cyber Tactics

IW has no precise definition, but scientists and researchers agree on its basic properties. IW is the tactic of using information sources to influence targets and make decisions that serve the interests of the IW perpetrator rather than their own. IW

gradually distorts people's perception of reality because the public does not know how to protect themselves (Glenn, et al., 2017). The other broad definition describes the use of technology in IW in two ways. A defensive way to maintain the required state or an offensive to change how the audience or adversary interprets the information they already have. (Bingle, 2023). The main goal of the IW is to collect information, manipulate it and then disseminate it. Disinformation and propaganda are the most effective tools. Social networks are becoming a primary digital resource for communicating and mobilising society and, in some cases, as a tool for conducting non-kinetic combat operations. Their exceptional characteristics, like almost unlimited reach, coupled with high information flow, speed, low cost, permanent availability, and, to a certain extent, anonymity, create ideal conditions for the spread of disinformation and propaganda. (Bialy, 2017). Disinformation and propaganda narratives aim to specifically influence the perception of social values or change political opinions to polarise society (Woolley, et al., 2018).

The IPSOS Institute conducted the study focused on specific factors and the extent of the influence of disinformation in individual European countries. It found that more than 29% of the population admitted to being significantly influenced by disinformation, and 55% believed that disinformation contained a specific photo (IPSOS, 2022). Additionally, a global survey of Internet users in 2023 found that 63% were willing to accept online privacy risks to make their lives more convenient (Petrosyan, 2024). Innovative technologies, particularly deep fakes, could pose a significant threat in this context. Figure 1 illustrates the importance of the Internet and social media in the context of global reach.

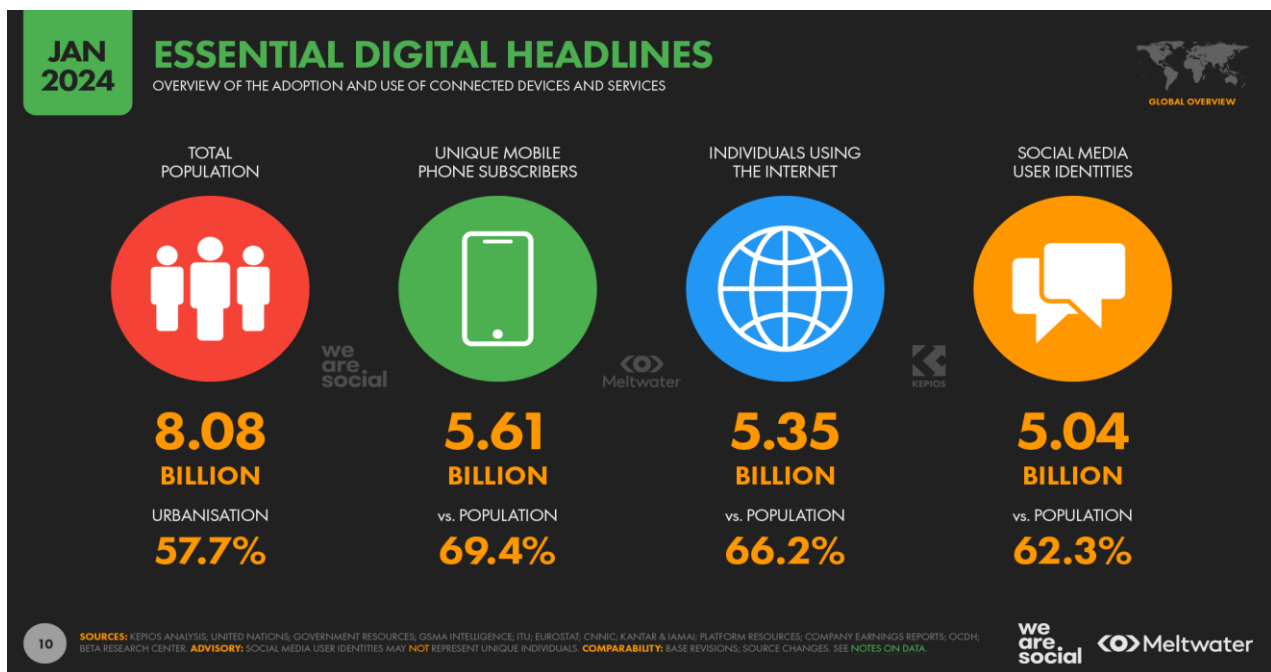


Figure 1: The state of digital in January 2024 (Kemp, 2024).

Some recent case studies can also help us better understand the consequences of IW. The Second Israel-Lebanon War in 2006 is a prime example of how Hezbollah used a variety of HW methods and tools, such as IW or psychological warfare (PW). Hezbollah conducted a massive global information campaign, broadcasting images and videos of destroyed cities, buildings, hospitals, schools, civilian deaths and suffering to media outlets around the world. This has earned Hezbollah public sympathy and criticism of Israel and its accusation of war crimes. (Ivančik, 2016). The same situation repeated itself after Hamas attacked Israel in 2023 and Israel's subsequent attacks on the Palestinian territories. During the invasion of Crimea, Russia used HW to minimise the use of conventional forces. It used the power of media and technology to mobilise its followers, demoralise the Ukrainian government and military, and justify its actions (Lange-Ionathamishvili, et al., 2015) (Unwala, 2015). In contrast, Russia's active measures in Ukraine failed in 2022. Russia's social media engagement, cyberattacks, propaganda and misinformation were largely ineffective or ignored. Ukraine's counter-campaign used social media to boost morale, expose Russian war crimes, mobilise global support, and even help raise money for defensive weapons (Kong, et al., 2022). CW also does not have a clear, generally accepted concept, and scientists have different definitions. 'Cyber-warfare is the sub-set of information warfare that involves actions taken within the cyber world.' (Parks, et al., 2011, p.122). Bokil sees this as using technology to carry out attacks on countries because of its effectiveness and ambiguity in the law (Bokil, 2023). For Pope, cyber warfare presents ethical challenges

and opportunities to enhance warfare practices, shaping emerging norms and standards and potentially leading to a more ethical state of war. (Pope, 2019). However, Smith views it as espionage and sabotage, which he does not perceive as acts of war (Smith, 2013). In response to the STUXNET worm's use, co-founder of Kaspersky Lab Eugene Kaspersky stated: 'This is the turning point, this is the time when we got to a really new world because in the past there were just cyber-criminals, now I am afraid it is the time of cyber-terrorism, cyber-weapons and cyber-wars.' (Kaspersky, 2010). Arquilla describes it as an information revolution with a new facet of national power, allowing less powerful actors to compete with great powers in a unipolar or multipolar world. (Arquilla, 2012). However, most science experts and scholars have reached a consensus on the definition of actors, which refers to state, state-sponsored and non-state actors. Today, the actors of cyber warfare are either non-state entities or even stateless persons (Bussolati, 2015), (Nur, et al., 2016), (Handler, 2022).

Today, modern technologies have already reached a stage that allows states to attack important strategic centres of their opponents via computer networks and to paralyse not just a tiny part of the country but the entire country. This type of warfare is less expensive than traditional warfare but still produces remarkable results and is becoming increasingly common. Scientists often see and distinguish three levels of cyber warfare. Human-level to change user behaviour. Software-enabled logical layer for espionage, adversarial computer attacks, and attacks on devices and installations within a physically controlled cyber domain. The physical layer disables or damages the hardware of the systems supporting cyberspace and forms the basis for the logical layer (Even, et al., 2012). High-tech capabilities that exchange, combine, and integrate real-time data are essential for advanced cyber domains. Technological innovations have enabled the cyber domain to grow significantly over the last two decades. The frequency, complexity, and impact of attacks in cyberspace have been such that NATO introduced cyber defence as part of its critical collective defence tasks at the 2014 Wales Summit. In this context, NATO recognised cyberspace as a new domain and cyber defence as a new priority at the 2016 Warsaw Summit (NATO, 2017).

The following examples show what effect a cyber-attack can have. Most reports say that a cyber-attack by the STUXNET worm on control systems of nuclear enriching installation has significantly compromised Iran's ability to produce nuclear weapons

(Baezner, et al., 2018). The Bronze Soldier Statue incident in Estonia 2007 involved multiple large-scale cyberattacks on media, banking, and government websites, resulting in massive denial-of-service attacks that overloaded the affected systems and forced them offline (Kozlowsky, 2013). The Russian cyber group Fancy Bear cyber-attack on Ukrainian artillery forces between 2014 and 2016 with Android application malware managed to identify the position data of the artillery units. As a result, more than 50% of Ukraine's artillery weapons were destroyed within two years (Paganini, 2016). During the initial phase of the invasion in February 2022, Russia launched hundreds of cyberattacks against the Ukrainian government and military institutions and networks. They also managed to penetrate the American ground equipment of the ViaSat communications network used by the Ukrainian military. This led to a significant communications blackout in the initial stages of the Russian invasion. (O'Neill, 2022). As we conclude this part, innovative capabilities that share, aggregate, and integrate real-time data are critical for advanced cyber domains. Technological advances have enabled CW to become the primary means of advancing information warfare manoeuvres rather than just a tool or means of conducting information warfare. Attacks are becoming more direct, efficient, broader, and quicker. Attackers have no name or face and operate in secret. They often use a fictitious ID or do not have one at all.

3. **There is an AI, a “New Piece on the Hybrid Chessboard“, with still unknown move options.**

4.

IW and CW are powerful HW tools, but combining them with AI radically expands the scale of HW's threats and capabilities. AI uses sophisticated algorithms to find trends, patterns, correlations, and best outcomes. It uses machine learning to predict more accurately and faster than human data analysts. The benefits of AI-powered predictive analytics are undeniable, and their integration into marketing and military strategies increases enormously. AI will make it possible to mimic, modify and change group behaviour, shaping hybrid conflicts' social and economic impacts (Thiele, 2020). According to Scharre, AI will revolutionise warfare in the 21st century like previous industrial revolutions. He identifies four battlefields for technology's impact on international affairs: talent, computers, institutions, and data. He emphasises that the interdependence of interactions between government, society, business, media, and science will be crucial to the governance of AI. It also recognises AI's threat to individual rights and human freedoms and the definition of reality and truth. In this context, he believes that democratic nations are less likely than totalitarian regimes to

exploit the full extent of AI capabilities (Scharre, 2023). Another major challenge is that the data used to drive AI algorithms can be limited, disputed, superficial, distorted, or easily manipulated by hostile actors. Artificial intelligence platforms are vulnerable to manipulation and deception when irregular conflicts occur in cyberspace or even sensor-rich physical domains (Egel, et al., 2019).

AI and machine learning systems require and depend on large volumes of data and large data sets. They require diverse data from a wide range of sources for reliable and effective algorithm deployment and use. The diagram in Figure 2 gives a better understanding of data volume.

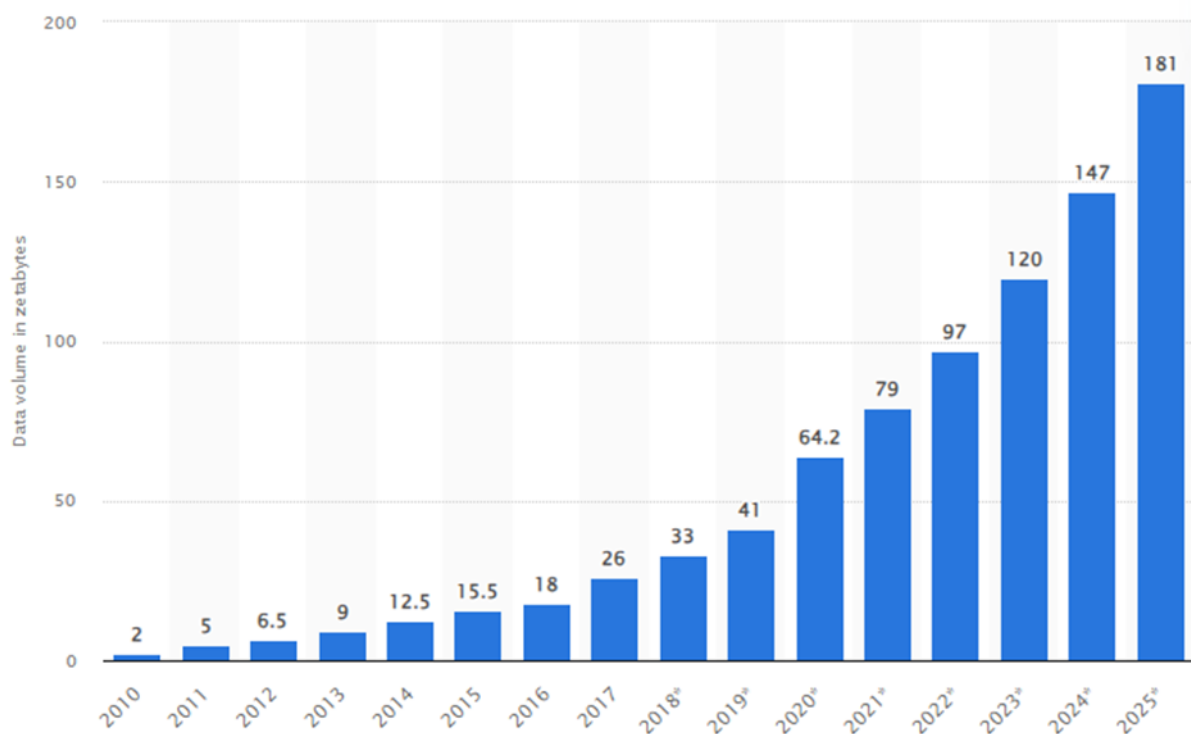


Figure 2: Data/information created, captured, copied, and consumed worldwide from 2010 to 2025 (Taylor, 2023).

Although AI has enormous potential, it is not a panacea. It is unlikely that AI will enhance influence and change group behaviour or the socioeconomic factors that contribute to irregular conflict, at least not in the next decade (Egel, et al., 2019). AI will undoubtedly increase the effectiveness of these initiatives by allowing them to process even more data and new sources, but 'Maneuver in the Human Domain Still Requires Humans.' (Egel, et al., 2019).

In summary, the use of communication and information technology in IW, together with the system-disruptive capabilities of CW, complemented by AI, has significant potential to multiply the disruptive effects of the attack, particularly regarding audience reach and public perception. Technological advances such as quantum computing, advanced detection, encryption and behavioural analysis combined with AI have led to significant growth in HW's unconventional capabilities. AI plays a crucial role in CW and IW tactics with synergistic effects. This triad is highly beneficial for various high-performance, low-risk HW operations that are changing the nature of current conflicts. Moreover, this technology still has the unexplored potential to revolutionise HW through a wide range of military applications and will undoubtedly add complexity to warfare.

4. “Brains over Muscles” - The new battlefield of minds in Hybrid Warfare.

In the context of new forms of HW, the cognitive domain is becoming increasingly important. One would say it is a novel combination of PW and IW with 21st-century technology, but quite the opposite. Cognitive warfare combines social, psychological, information technology, and cyber engineering capabilities to target individuals, specific groups, or a massive portion of society. However, the fundamental difference is that in the past, it was a complementary form of physical military conflict; after the Second World War, we also encountered it as the primary military strategy (Pivka, 2019). This type of warfare is an organised persuasion process that uses methods to attack the areas the weapons cannot hit to influence the opponent (Taylor, 2003). This perspective sees it as using digital technologies for psychological and informational operations.

Nevertheless, cognitive warfare differs significantly from the ideas mentioned above in many ways, in that everyone usually participates in information processing and knowledge creation unintentionally. In the past, individuals were influenced and passively submitted to adversary propaganda, but now, they unconsciously and actively contribute to it (Du Cluzel, 2021). The NATO Review describes cognitive warfare as limited, with brief time horizons focused on specific impacts or long-term strategic campaigns to destroy entire societies or alliances over decades. It also claims: ‘In cognitive warfare, the human mind becomes the battlefield. The aim is to change what people think and how they think and act...In its extreme form, it has the

potential to fracture and fragment an entire society so that it no longer has the collective will to resist an adversary's intentions.' (NATO, 2021). A similar Du Cluzel argues: 'With the growing role of technology and information overload, individual cognitive abilities will no longer be sufficient to ensure an informed and timely decision-making, leading to the new concept of Cognitive Warfare, which has become a recurring term in military terminology in recent years.' (Du Cluzel, 2020, p 1).

There are also different doctrinal and conceptual approaches to cognitive warfare. The Western approach tends towards a technical-scientific perspective, emphasising using biotechnologies and neuroscience as weapons (Giordano, 2017). The new techniques also include complex social manipulations with the aim of not only fighting for your brain but also turning every person into a weapon. (Norton, 2021). The Russian approach to cognitive warfare exploits the synergistic effect of CW and IW. Russia also uses measures of "reflexive control" in combination with communication technologies, media, and disinformation campaigns to manipulate public perception, undermine trust and destabilise political systems (Danet, 2023). The Chinese perspective of the cognitive domain in HW use is divided into two categories, focusing on synergies between brain science, AI, and biotechnology. The first includes devices that affect a person's ability to think and reason. The second includes technologies influencing a person's subconscious feelings, thoughts, knowledge, and willpower (Beauchamp, 2019), (Kania, 2020).

Cognitive warfare bypasses the conventional battlefield. It is not a fight against what we think but against how we think. Its main advantage is its moral justification due to the lack of legal sanctions, and weaknesses in our information and decision-making processes are still ignored. In summary, 'As future conflicts continue to devolve into wars of thinking men, in a race to outthink and outlearn an adaptable adversary, NATO will also have to adapt.' (Davis, 2015). This time has already come, and technological advances, particularly in brain research, reveal unprecedented possibilities in the cognitive domain, requiring a more active approach and leading to threats that embody broader thinking. It presents new challenges to the military, which must master integrating passive and active forms of cognitive neuroscience and AI technology in novel approaches to ensure cognitive security.

5. Even Less Light into the Grey Zone

HW and GZ's ideas are nothing new and present long-standing military tactics. 'They manoeuvre in the ambiguous no-man's-land between peace and war, reflecting the sort of aggressive, persistent, determined campaigns characteristic of warfare but without the overt use of military force.' (Mazarr, 2015). What is new is the massive exploitation of information technology, which offers significant anonymity, new adversaries, and the scientifically based use of new vulnerabilities to achieve a result. Computer and communications technologies are so important that they have become weapons platforms, and software become ammunition. Furthermore, innovative technology in GZ goes beyond the political and military operations that adversaries often employ, including trade and diplomacy (ISAB, 2017). Votel and his collective offer a similar definition, adding fierce competition in politics, economics, information, and military power that is more aggressive than traditional interstate diplomacy but more restrained than open conventional warfare (Votel, et al., 2016).

Mazarr claims these strategies are nothing new and considers them gradualist and erosive techniques for incremental gains and attempts to prevent escalation into open conventional conflict (Mazarr, 2015). This theory also supports Paul, who claims that these actions aim for the attacker to achieve his goals in tiny increments without ever eliciting a significant response (Paul, 2016). However, it should be noted that the GZ strategy also has a clear disadvantage. While it allows players to exploit others' weaknesses, it does not guarantee they will achieve remarkable results. Applying the GZ strategies like the salami method will not guarantee ultimate goals if opponents are sufficiently resilient. This argument supports a team of authors who say that GZ involves coercive measures to change the status quo, typically leading to a conventional military response. In symmetrical conflicts, there is a high probability to achieve the goal through unconventional means. On the other hand, in asymmetric conflicts, combining conventional and unconventional methods is an obvious choice (Carment, et al., 2018). The current state of the conflict in Ukraine shows how serious the international, economic, and military consequences of crossing the threshold into war can be. Therefore, GZ techniques may also be attractive for many countries due to their relative weakness. Their GZ tactics often show strong influence and power but can also blur a fundamental inability to take kinetic tactics or use conventional forces.

For example, China's current conventional military power and Russia's economic power could prevent them from achieving their regional or strategic objectives and force them to resort to GZ operations.

Modern technologies have given actors new tools with greater flexibility, making them more demanding and unpredictable. Also, with the availability of dual civil and military use of new technological tools and their creative combination, a wider range of actors expands specific methods depending on the symmetry of the conflicting participants. The conflict actors in the GZ rely primarily on unconventional tactics that include long-term strategic goals and international rivalry but do not exceed the threshold of formal aggression. We can conclude that hybrid war and GZ conflict are fundamentally different concepts at the strategic level. Using tactical effect sequences, HW combines conventional and unconventional tactics to achieve strategic levels. From the above, one can deduce that hybrid wars are a subset of GZ conflicts. However, using separate unconventional GZ methods may not be the most effective solution to achieve the strategic goal.

6. Blurring of Peace and War

Several authors argue that traditional Western ideas about warfare are at odds with the 21st-century notion of modern warfare. They argue that a significant paradigm shift occurred due to the emergence of a unipolar world order after the Cold War. Some authors describe hybrid war as a new brand, an asymmetrical war, or 'old wine in new bottles.' (Weissmann, 2019). So, let us look at how hybrid war relates to classic war.

A serious discussion about the nature and character of war requires considering the perspective of two masters of military strategy. Carl von Clausewitz's most well-known definition is, 'War is thus an act of violence to compel our enemy to do our will.' (Clausewitz, n.d.). In this sense, an act of violence is using violence through military force to destroy enemy forces and achieve victory on the battlefield. On the other hand, he argues that war is not a single and independent activity but merely a 'continuation of policy by other means.' (Clausewitz, n.d.). He also describes the uniqueness of war, which has other peculiarities such as friction, fear, violence, passion, and emotions, and that even crossing these boundaries leads to war. Considering this statement, such a conflict in the GZ is not an act of war in the narrow sense but in a general form. Sun Tzu offers a much more precise understanding of the basics of HW, stating, 'Thus those skilled in war subdue the enemy's army without battle.' (Tzu, 1963, p.79). Tzu

reflects on the strategic concept of war regarding effective tactical manoeuvres and deployment of troops on the battlefield. However, his vision of using military force is at the lower end of the spectrum. Achieving the desired result is also possible by avoiding combat in the face of the disproportionality of military force, deception or influencing the enemy. The conclusion from analysing the approaches of these strategists to the definition of war is that both consider war as any military or political activity aimed at enforcing their will or making a profit at the expense of the enemy. However, can we still call it war without defined military conflicts, a recognisable battlefield, or military involvement as part of a political campaign or propaganda?

According to researchers, HW can prevent or deter conventional conflicts by requiring complex responses, employing a balanced force strategy that may deter adversaries, and adding ambiguity and complexity to international relations (Miller, 2015), (Wither, 2016) and (Weissmann et al., 2021). War can also be hybrid peace when it meets the criteria of crisis, internal conflict, and local or regional war (Perepelytsia, 2021). Therefore, HW that does not exceed the war threshold can be perceived as peace. This argument supports a white paper of the USSOCOM saying that, in the history of U.S. military operations, only five of fifty-seven conflicts were officially declared wars, with others balancing in the GZ (USSOCOM, 2015). Army General Gerasimov takes the opposite view on the perception of HW, describing it as a new generation of wars where hybrid ones substitute traditional military approaches and procedures through a wide range of international and humanitarian aspects, including political, economic, informational, and other instruments (Gerasimov, 2016). McCuen claims that a hybrid war is a war with a conventional form, but the decisive battles take place on asymmetrical battlefields rather than conventional ones (McCuen, 2008). Furthermore, Gerasimov notes that in the 21st century, the boundaries between war and peace are becoming increasingly blurry; wars do not start with a declaration of war; they start with different forms of conflict and do not have a usual pattern (Gerasimov, 2016).

From a legal perspective, states involved in conflicts in the GZ are not at war (Bothwell, 2021). International agreements relating to wartime, such as the UN Charter and the Geneva Conventions, do not extend their authorisations or protections to situations that fall within the GZ. International law has no tailor-made rules except the Budapest Convention on Cybercrime. This situation requires a new conceptual approach and definition of new forms of war and the use of law and strategy - especially by state

actors (Ball, 2023). However, the Tallinn Manual states: 'A cyber operation constitutes a use of force when its scale and effects are comparable to non-cyber operation rising to the level of a use of force.' (Schmitt, 2017). It is also essential that at the Wales Summit in 2014, NATO leaders recognised that the impact of cyber-attacks can be as damaging to our society as a conventional attack and agreed that a cyber-attack on one of their members is an attack on the entire alliance, and therefore trigger a military response (NATO, 2014).

Considering all the above points and Schmid's argument, 'All war is hybrid, but there is also a specific hybrid way of conducting war' (Schmid, 2019). I conclude this paragraph by arguing that using various strategies, forms, techniques, and procedures that fit into the framework of a hybrid war is just a modern means to avoid a direct confrontation with the enemy, that is, a conventional war. This does not mean that it is not a war. In this sense, one can also conclude that the HW is still war and GZ is just a battlefield where these modern tactics ensure the activity's secrecy, concealing identity and perception of supporting the enemy.

Recommendations

It is important to note that new technologies have expanded not only the range of options for the attacker but also the resources and capabilities of the defender. Policymakers and military strategists must adopt a more holistic and adaptive approach rather than the old, linear approach and develop comprehensive strategies that leverage all available resources and capabilities. The crucial challenge of the current time is the deliberate synergistic effects of current HW concepts and forms and rapid adaptation to evolving threats of innovative technologies. A country should prioritise the protection of critical systems and vital national infrastructures and ensure the security of other aspects of the economy and society. New artificial intelligence tools will soon manipulate the human mind and alter human behaviour. Proper defence requires awareness of the ongoing HW campaign. It requires recognising, observing, and integrating human situational awareness into traditional situational awareness before acting. Therefore, a comprehensive study investment and collaboration of innovative technologies such as cognitive science, nanotechnology, biotechnology, and AI and their integration into military operations is inevitable. AI-powered tools play a crucial role in exercises and training essential to combat hybrid attacks in the military,

government, and civilian institutions. Data availability, reliability, processing capability and protection are essential components. Security and defence organisations should develop closer relationships with civilian industry due to the significant resource and data availability in the private sector. This collaboration is beneficial and necessary for our defence planning and underscores its urgency. An example of a recent NATO initiative is The Defence Innovation Accelerator for the North Atlantic, which connects defence sector end users with established technological pioneers in industry, academia, and start-ups to develop technological solutions. Countries must remain at the forefront of technological development, invest in education and training, and promote international cooperation to manage hybrid warfare's complex and ever-changing terrain effectively. The fundamental element of success is the international exchange of information, experiences, and procedures among NATO, the EU, and particular states. Unless NATO makes continuous, proactive and sustained advances in cyber and cognitive domains against advanced and adaptive adversaries, kinetic conflict will be the only option. Non-kinetic forms of HW have made significant progress and have become increasingly common since their introduction. Development and its changes have not yet reached their final form, and continuous studies are needed to understand better the threats they pose and to counter their future forms effectively.

Conclusion:

In conclusion, recent technologies, advanced systems, and novel, non-traditional methods in HW are part of the dynamic progress in the military and society. The worsening global economic, social, environmental and security problems will make this type of war prevalent in the coming decades, highlighting the importance of the cyber and emerging cognitive domains. The development of technology has changed the way of waging wars in many ways. Significantly extended the tools and actors in the grey zone, increased ambiguity, and blurred the lines between peace and war. In today's multipolar world, it will not be possible to quickly identify the diverse technological threats and actors due to their illegal or irregular tactics, anonymity and diverse interests. The availability and anonymity of digital technologies mean that more activities are shifting to cyberspace, enabling quick and easy fulfilment of goals with minimal risk of punishment. There is still no answer to the question of what sovereignty and territorial integrity in the cyber domain mean. Therefore, adopting a legal definition of HW and GZ conflicts is also an inevitable step in facilitating the effective countering

of hybrid attacks. Undoubtedly, new wars will be more about perception and influence than weapons, and the cognitive domain will be the main battlefield. Neuroattacks on the brain are not considered conventional attacks under international law, and neither are they considered biological weapons. State and country can be refuted by changing society's perception, opinion, goals, personal values and priorities. Destroyed infrastructure can be restored, but a mindset change is almost irreversible. It is also important to mention that those who are able to keep and process data will run the future world of digital order and shape what we want, what we think, and what we do. HW is changing the nature of the conflict, where borders no longer guarantee security, and the increasing potential of cyberspace brings more complexity to defence planning. Regardless of the HW's ambiguity, the war is still a war. Like all forms of warfare, HW fundamental is violence, and its goal is the same: to use organised physical or psychological violence or the threat to your opponent.

Bibliography

Abbott, Daniel H. 2010. The Handbook of 5GW. *www.dokumen.pub*. [Online] 13 July 2010. [Cited: 21 April 2024.] <https://dokumen.pub/the-handbook-of-fifth-generation-warfare-9781934840177-1934840173.html>.

Arquilla, John. 2012. Cyberwar Is Already Upon Us. *https://foreignpolicy.com/*. [Online] 27 February 2012. [Cited: 21 April 2024.] <https://foreignpolicy.com/2012/02/27/cyberwar-is-already-upon-us/>.

Baezner, Marie and Robin , Patrice. 2018. Stuxnet. *https://www.researchgate.net*. [Online] February 2018. [Cited: 21 April 2024.] https://www.researchgate.net/publication/323199431_Stuxnet.

Ball, Joshua. 2023. The Changing Face of Conflict: What is Hybrid Warfare? *https://globalsecurityreview.com*. [Online] 2023. [Cited: 22 April 2024.] <https://globalsecurityreview.com/hybrid-and-non-linear-warfare-systematically-erases-the-divide-between-war-peace/>.

Beauchamp, Nathan Mustafaga. 2019. Cognitive Domain Operations: The PLA's New Holistic Concept for Influence Operations. *https://jamestown.org*. [Online] 6 September 2019. [Cited: 22 April 2024.] <https://jamestown.org/program/cognitive-domain-operations-the-plas-new-holistic-concept-for-influence-operations/>.

Bialy, Beata. 2017. Social Media-From Social Exchange to Battlefield. *https://cyberdefensereview.army.mil/*. [Online] 2017. [Cited: 21 April 2024.] https://cyberdefensereview.army.mil/Portals/6/Documents/CDR%20Journal%20Articles/Social%20Media%20From%20Social%20Exchange_Bialy.pdf?ver=2018-07-31-093711-437.

Bilal, Arsalan. 2021. Hybrid Warfare-New Threats, Complexity, and “Trust” as the Antidote. *www.nato.int*. [Online] 30 November 2021. [Cited: 21 April 2024.] <https://www.nato.int/docu/review/articles/2021/11/30/hybrid-warfare-new-threats-complexity-and-trust-as-the-antidote/index.html>.

Bingle, Morgan. 2023. What is Information Warfare? <https://jsis.washington.edu/>. [Online] 25 September 2023. [Cited: 21 April 2024.] <https://jsis.washington.edu/news/what-is-information-warfare/>.

Bokil, Rohit. 2023. Cyber Warfare: Taking War to Cyberspace and its Implications for International humanitarian Law. <https://www.ijfmr.com/>. [Online] February 2023. [Cited: 21 April 2024.] <https://www.ijfmr.com/papers/2023/1/1494.pdf>.

Bothwell, Heather M. 2021. Gray Is the New Black: A Framework to Counter Gray Zone Conflicts. <https://ndupress.ndu.edu>. [Online] 31 March 2021. [Cited: 22 April 2024.] <https://ndupress.ndu.edu/Media/News/News-Article-View/Article/2556217/gray-is-the-new-black-a-framework-to-counter-gray-zone-conflicts/>.

Bussolati, Nicollo. 2015. The Rise of Non-State Actors in Cyberwarfare. <https://www.academia.edu/>. [Online] Oxford University Press, 2015. [Cited: 21 April 2024.] https://www.academia.edu/24359488/The_Rise_of_Non_State_Actors_in_Cyberwarfare.

Carment, David and Belo, Dani. 2018. War's Future: The Risks and Rewards of Grey Zone Conflict and Hybrid Warfare. <https://www.researchgate.net>. [Online] October 2018. [Cited: 22 April 2024.] https://www.researchgate.net/publication/334959464_War's_Future_The_Risks_and_Rewards_of_Grey_Zone_Conflict_and_Hybrid_Warfare.

Clausewitz, Carl von. n.d.. On War. <https://clausewitzstudies.org>. [Online] transl. by John Graham, n.d. [Cited: 22 April 2024.] <https://clausewitzstudies.org/readings/OnWar1873/TOC.htm>.

Danet, Didier. 2023. Cognitive Security: Facing Cognitive Operations in Hybrid Warfare. <https://papers.academic-conferences.org>. [Online] Jun 2023. [Cited: 22 April 2024.] <https://papers.academic-conferences.org/index.php/eccws/article/view/1442/1160>.

Davis, John R. 2015. Continued Evolution of Hybrid Threats. <https://www.jwc.nato.int>. [Online] 2015. [Cited: 22 April 2024.] https://www.jwc.nato.int/images/stories/threeswords/CONTINUED_EVOLUTION_OF_HYBRID_THREATS.pdf.

Du Cluzel, Francois. 2020. Cognitive Warfare, a Battle for the Brain. <https://www.sto.nato.int>. [Online] November 2020. [Cited: 22 April 2024.] [https://www.sto.nato.int/publications/STO%20Meeting%20Proceedings/STO-MP-HFM-334/\\$MP-HFM-334-KN3.pdf](https://www.sto.nato.int/publications/STO%20Meeting%20Proceedings/STO-MP-HFM-334/$MP-HFM-334-KN3.pdf).

Du Cluzel, Francois. 2021. NATO Innovation Challenge Fall 2021: Cognitive Warfare. *youtube.com*. [Online] 2021. [Cited: 22 April 2024.] https://www.youtube.com/watch?v=LOVBJXCL_s.

Egel, Daniel, Robinson, Eric and Cleveland, Charles. 2019. AI and Irregular Warfare: An Evolution, Not a Revolution. <https://warontherocks.com>. [Online] 31 October 2019. [Cited: 22 April 2024.] <https://warontherocks.com/2019/10/ai-and-irregular-warfare-an-evolution-not-a-revolution/>.

Even , Shmuel and Siman-Tov, David. 2012. Cyber Warfare: Concepts and Strategic Trends. <https://www.files.ethz.ch/>. [Online] 1 May 2012. [Cited: 21 April 2024.] https://www.files.ethz.ch/isn/152953/inss%20memorandum_may2012_nr117.pdf.

Gerasimov, Valery. 2016. The Value of Science is in the Foresight New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations. armyupress.army.mil. [Online] January-February 2016. [Cited: 21 April 2024.] https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/MilitaryReview_20160228_art008.pdf.

Giordano, James. 2017. Weaponizing the Brain: Neuroscience Advancements Spark Debate. <https://www.nationaldefensemagazine.org/>. [Online] 11 May 2017. [Cited: 22 April 2024.] <https://www.nationaldefensemagazine.org/articles/2017/5/11/weaponizing-the-brain-neuroscience-advancements-spark-debate>.

Glenn, Jerome C., Florescu, Elizabeth and Milenium project team. 2017. State of The Future V. 19.0. <https://millennium-project.org/>. [Online] 2017. [Cited: 21 April 2024.] https://millennium-project.org/wp-content/uploads/2017/10/SOF2017-ExecSumm-front_matter.pdf.

Handler, Simon. 2022. The 5x5—Non-state armed groups in cyber conflict. <https://www.atlanticcouncil.org>. [Online] 26 October 2022. [Cited: 21 April 2024.] <https://www.atlanticcouncil.org/content-series/the-5x5/the-5x5-non-state-armed-groups-in-cyber-conflict/>.

IPSOS. 2022. More than a quarter of the Central European and Baltic population is strongly affected by disinformation. <https://www.ipsos.com/>. [Online] 2022. [Cited: 21 April 2024.] <https://www.ipsos.com/cs-cz/more-quarter-central-european-and-baltic-population-strongly-affected-disinformation>.

ISAB . 2017. Report on Gray Zone Conflict. <https://2009-2017.state.gov/>. [Online] International Security Advisory Board, 3 January 2017. [Cited: 22 April 2024.] <https://2009-2017.state.gov/documents/organization/266849.pdf>.

Ivančík, Radoslav. 2016. Theoretical background for the research of problem of the hybrid war-the war of the 21. century. <https://fmv.euba.sk/>. [Online] Faculty of International Relations, University of Economics in Bratislava, 15 Jun 2016. [Cited: 21 April 2024.] https://fmv.euba.sk/www_write/files/dokumenty/veda-vyskum/medzinarodne-vztahy/archiv/2016/MV_2016_2_130-156_Ivancik.pdf.

Kania, Elisa B. 2020. Minds at War China's Pursuit of Military Advantage through Cognitive Science and Biotechnology. <https://ndupress.ndu.edu>. [Online] 20 January 2020. [Cited: 22 April 2024.] <https://ndupress.ndu.edu/Media/News/News-Article-View/Article/2053585/minds-at-war-chinas-pursuit-of-military-advantage-through-cognitive-science-and/>.

Kaspersky, Eugen. 2010. Kaspersky Lab provides its insights on Stuxnet worm. <https://www.kaspersky.com/>. [Online] 24 September 2010. [Cited: 21 April 2024.] https://www.kaspersky.com/about/press-releases/2010_kaspersky-lab-provides-its-insights-on-stuxnet-worm.

Kemp, Simon. 2024. Global Overview Report Pictures: The state of digital in January 2024. [Digital image]. <https://datareportal.com/>. [Online] Datareportal, 31 January 2024. [Cited: 21 April 2024.] <https://datareportal.com/reports/digital-2024-global-overview-report>.

Kong , Weilong and Marler , Timothy. 2022. Ukraine's Lessons for the Future of Hybrid Warfare. <https://www.rand.org/>. [Online] 28 November 2022. [Cited: 21 April 2024.] <https://www.rand.org/pubs/commentary/2022/11/ukraines-lessons-for-the-future-of-hybrid-warfare.html>.

Kozlowsky, Andrzej. 2013. Comparative Analysis of Cyberattacks on Estonia, Georgia and Kyrgyzstan. <https://www.researchgate.net/>. [Online] European Scientific Institute, December 2013. [Cited: 21 April 2024.] https://www.researchgate.net/profile/Nnedinma-Umeokafor/publication/260107032_International_Scientific_Forum_ISF_2013vol3/links/02e7e52f964505c201000000/International-Scientific-Forum-ISF-2013vol3.pdf#page=246.

Krishan, Armin. 2022. Fifth Generation Warfare, Hybrid Warfare, and Gray Zone Conflict: A Comparison. <https://thescholarship.ecu.edu/>. [Online] 2022. [Cited: 21 April 2024.] <https://thescholarship.ecu.edu/bitstream/handle/10342/12401/KrishnanFifthGenerationWarfareHybridWarfareandGrayZoneConflict.pdf?sequence=1>.

Lamey, Donny. 2023. The Evolution of Technology: Past, Present and Future. . www.discovertec.com. [Online] 13. October 2023. [Cited: 21. April 2024.] <https://www.discovertec.com/blog/evolution-of-technology>.

Lange-Ionatamishvili , Elina and Svetoka, Sandra. 2015. Strategic Communications And Social Media in the Russia Ukraine Conflict. <https://ccdcoe.org/>. [Online] CCDCOE, 2015. [Cited: 21 April 2024.] https://ccdcoe.org/uploads/2018/10/Ch12_CyberWarinPerspective_Lange_Svetoka.pdf.

Mazarr , Michael J. 2015. Mastering the Grey Zone: Understanding a Changing Era of Conflict. <https://press.armywarcollege.edu>. [Online] US Army War College , 1 December 2015. [Cited: 22 April 2024.] <https://press.armywarcollege.edu/cgi/viewcontent.cgi?article=1427&context=monographs>.

McCuen, Josh J. 2008. Hybrid Wars. <https://www.armyupress.army.mil>. [Online] April 2008. [Cited: 22 April 2024.] https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/MilitaryReview_20080430_art017.pdf.

Miller, Michael. 2015. Hybrid Warfare: Preparing for Future Conflicts. <https://apps.dtic.mil>. [Online] 17 February 2015. [Cited: 22 April 2024.] <https://apps.dtic.mil/sti/pdfs/ADA618902.pdf>.

NATO. 2021. Brussel Summit Communiqué. *www.nato.int*. [Online] 14 Jun 2021. [Cited: 21 April 2024.] https://www.nato.int/cps/en/natohq/news_185000.htm.

NATO. 2021. Countering Cognitive Warfare: Awareness and Resilience. *https://www.nato.int/*. [Online] Johns Hopkins University & Imperial College London, 20 May 2021. [Cited: 22 April 2024.] <https://www.nato.int/docu/review/articles/2021/05/20/countering-cognitive-warfare-awareness-and-resilience/index.html>.

NATO. 2014. Wales Summit Declaration. *https://www.nato.int*. [Online] 5. September 2014. [Cited: 23. April 2024.] https://www.nato.int/cps/en/natohq/official_texts_112964.htm.

NATO. 2017. Warsaw Summit key decisions. *https://www.nato.int/*. [Online] February 2017. [Cited: 21 April 2024.] https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2017_02/20170206_1702-factsheet-warsaw-summit-key-en.pdf.

Norton, Ben. 2021. Behind NATO's 'cognitive warfare': 'Battle for your brain' waged by Western militaries. *https://mronline.org/*. [Online] 13 October 2021. [Cited: 22 April 2024.] <https://mronline.org/2021/10/13/behind-natos-cognitive-warfare-battle-for-your-brain-waged-by-western-militaries/>.

Nur , Kamile Servis and Seker , Ensar. 2016. Cyber Warfare: Terms, Issues, Laws and Controversies. *https://www.researchgate.net*. [Online] July 2016. [Cited: 21 April 2024.] https://www.researchgate.net/publication/306064145_Cyber_warfare_terms_issues_laws_and_controversies.

O'Neill , Patrick Howell. 2022. Russia Hacked an American Satellite Company One Hour before the Ukraine Invasion. *https://www.technologyreview.com*. [Online] 10 May 2022. [Cited: 21 April 2024.] <https://www.technologyreview.com/2022/05/10/1051973/russia-hack-viasat-satellite-ukraine-invasion/>.

Paganini, Pierluigi. 2016. Fancy Bear Apt Tracked Ukrainian Artillery Units With an Android Implant. *https://securityaffairs.com/*. [Online] 22 December 2016. [Cited: 21 April 2024.] <https://securityaffairs.com/54635/cyber-warfare-2/implant-ukrainian-artillery-units.html>.

Parks , Raymond C. and Duggan, David P. 2011. Principles of Cyber-warfare. *https://www.researchgate.net/*. [Online] November 2011. [Cited: 21 April 2024.] https://www.researchgate.net/publication/224259524_Principles_of_Cyberwarfare.

Patel, Asmaa. 2019. Fifth-Generation Warfare and the Definitions of Peace. *https://journals.lib.sfu.ca*. [Online] 22 November 2019. [Cited: 21 April 2024.] <https://journals.lib.sfu.ca/index.php/jicw/article/view/1061/3074>.

Paul, Christopher. 2016. Confessions of a Hybrid Warfare Skeptic. *https://smallwarsjournal.com*. [Online] 3 March 2016. [Cited: 22 April 2024.] <https://smallwarsjournal.com/jrnl/art/confessions-of-a-hybrid-warfare-skeptic>.

Perepelytsia, Hryhorii. 2021. The Dilemma Of War And Peace In The Trend Of The XXI Century (Russian – Ukrainian case). <https://repozytorium.amu.edu.pl>. [Online] Taras Shevchenko National University of Kyiv, 2021. [Cited: 22 April 2024.] <https://repozytorium.amu.edu.pl/server/api/core/bitstreams/efa9a9bc-6b47-4d57-a568-48c230390f22/content>.

Petrosyan, Ani. 2024. Global users accepting online privacy risks for convenience 2023, by country. <https://www.statista.com/>. [Online] Statista, 23 January 2024. [Cited: 21 April 2024.] <https://www.statista.com/statistics/1023952/global-privacy-risks-accept-convenience-convenience/>.

Pivka, Adrian. 2019. Psychologická vojna – rešerš odbornej literatúry. <https://is.muni.cz/>. [Online] 5 May 2019. [Cited: 22 April 2024.] https://is.muni.cz/th/modmr/bakalarka_pivka.pdf.

Pope , Billy Jr. E. 2019. A Better State of War Surmounting the Ethical Cliff in Cyber Warfare. <https://media.defense.gov/>. [Online] Air University Press. Maxwell AFB, Alabama, February 2019. [Cited: 21 April 2024.] https://media.defense.gov/2019/Feb/07/2002087422/-1/-1/0/DP_0029_POPE_BETTER_STATE_OF_WAR.PDF.

Scharre, Paul. 2023. *Four Battlegrounds Power in The Age of Artificial Intelligence*. New York : W.W. Norton, 2023. ISBN 978-0-393-86686-5.

Schmid, Johan. 2019. The Hybrid Face of Warfare in the 21st Century. The Hybrid Face of Warfare in the 21st Century. <https://www.maanpuolustus-lehti.fi>. [Online] 7 March 2019. [Cited: 22 April 2024.] <https://www.maanpuolustus-lehti.fi/the-hybrid-face-of-warfare-in-the-21st-century/>.

Schmitt, Michael N. (Ed.). 2017. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. <https://www.cambridge.org>. [Online] Cambridge University Press, February 2017. [Cited: 22 April 2024.] <https://www.cambridge.org/core/books/tallinn-manual-20-on-the-international-law-applicable-to-cyber-operations/E4FFD83EA790D7C4C3C28FC9CA2FB6C9>.

Smith, Troy. 2013. Cyber Warfare:A Misrepresentation of the True Cyber Threat. <https://www.researchgate.net/>. [Online] American Intelligence Journal, January 2013. [Cited: 21 April 2024.] https://www.researchgate.net/publication/280204557_Cyber_Warfare_A_Misrepresentation_of_the_True_Cyber_Threat.

Taylor, Petroc. 2023. Volume of data/information created, captured, copied, and consumed worldwide from 2010 to 2025. [Digital image]. <https://www.statista.com/>. [Online] Statista, 16. November 2023. Cited: 21 April 2024.] <https://www.statista.com/statistics/871513/worldwide-data-created/>.

Taylor, Philip M. 2003. Munition of the mind. <https://web.archive.org/>. [Online] Manchester University Press, 2003. [Cited: 22 April 2024.] https://web.archive.org/web/20180423183330id_/http://web.elastic.org/~fche/mirrors/www.jya.com/2013/01/aaron-swartz/Mind-Munitions.pdf.

Thiele, Ralph D. and Schmid, Johan. 2020. Hybrid Warfare – Orchestrating the Technology Revolution. <https://css.ethz.ch/>. [Online] January 2020. [Cited: 21 April

2024.] https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/resources/docs/ISPSW_663_Thiele_Schmid.pdf.

Thiele, Ralph D. 2020. Artificial Intelligence – A key enabler of hybrid warfare. <https://www.hybridcoe.fi>. [Online] Hybrid CoE, March 2020. [Cited: 21 April 2024.] https://www.hybridcoe.fi/wp-content/uploads/2020/07/WP-6_2020_rgb-1.pdf.

Thiele, Ralph D. 2021. Hybrid Warfare Future and Technologies. <https://ebookcentral.proquest.com/>. [Online] 2021. [Cited: 21 April 2024.] <https://ebookcentral.proquest.com/lib/mil/reader.action?docID=6801312>.

Tzu, Sun. Samuel B. Griffith 1963. *The art of war*. New York : Oxford University Press, Samuel B. Griffith 1963.

Unwala, Azhar. 2015. Brandishing the Cybered Bear: Information War and the Russia-. <https://www.researchgate.net/>. [Online] Georgetown University, December 2015. [Cited: 21 April 2024.] https://www.researchgate.net/publication/307916803_Brandishing_the_Cybered_Bear_Information_War_and_the_Russia-Ukraine_Conflict.

USSOCOM. 2015. White Paper: The Grey Zone. <https://info.publicintelligence.net>. [Online] 9 September 2015. [Cited: 22 April 2024.] <https://info.publicintelligence.net/USSOCOM-GrayZones.pdf>.

Votel , Joseph L., et al. 2016. Unconventional Warfare in the Gray Zone. <https://ndupress.ndu.edu>. [Online] 2016. [Cited: 22 April 2024.] https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-80/jfq-80_101-109_Votel-et-al.pdf.

Weissmann, Mikael. 2019. Hybrid warfare and hybrid threats today and tomorrow: Towards an analytical framework. <https://www.diva-portal.org>. [Online] 30 April 2019. [Cited: 22 April 2024.] https://www.researchgate.net/publication/334967002_Hybrid_warfare_and_hybrid_threats_today_and_tomorrow_towards_an_analytical_framework

Weissmann, Mikael, et al. 2021. Hybrid Warfare: Security and Asymmetric Conflict in International Relations. <https://www.researchgate.net>. [Online] January 2021. [Cited: 22 April 2024.] https://www.researchgate.net/publication/334967002_Hybrid_warfare_and_hybrid_threats_today_and_tomorrow_towards_an_analytical_framework

Wither, James K. 2016. Making Sense of Hybrid Warfare. <https://www.jstor.org>. [Online] 2016. [Cited: 22 April 2024.] <https://www.jstor.org/stable/26326441>.

Woolley, Samuel C: and Howard , Philip N. 2019. Computational Propaganda. <https://books.google.ee/>. [Online] Oxford University Press, 2019. [Cited: 21 April 2024.] https://books.google.ee/books?hl=sk&lr=&id=qTpxDwAAQBAJ&oi=fnd&pg=PP1&dq=Howard,+P.+N.,+Woolley,+S.2018:&ots=fpH7UrwhPd&sig=YDRi3TpjOrbHKXciqJeqULrQ6lE&redir_esc=y#v=onepage&q=Howard%2C%20P.%20N.%2C%20Woolley%2C%20S.2018%3A&f=false.

RIMGAUDAS GAMULIS. Lithuania's critical infrastructure protection: national and EU approaches

Introduction

In the digital age, cyberspace is becoming a crucial component of national security for any country. Similar to how the human nervous system depends on particular critical pathways to function (Porges, 2009), cyberspace, which is made up of interconnected communication networks, information technology systems, and electronic data (NSO, 2020), due to its strategic importance, vulnerability and interdependence with the physical environment is processing as one of the most critical factors for state's social development, economic growth and national security (Medeiros et al., 2020).

Cyberspace is an expansive domain, and various elements coexist; however, despite this complexity, critical infrastructure is a vital terrain (Pantin, 2017) that serves as the backbone for communication, governance, defence, and national security. The contemporary landscape of critical infrastructure has changed significantly. Today, critical infrastructure rarely exists or functions in isolation, and it is becoming a more tightly coupled, interconnected, and interactive environment that creates a complex formation that generally includes the interplay between critical information infrastructure and national information infrastructures (Figure 1). In broad terms, critical infrastructure encompasses the nation's essential systems across diverse sectors. In contrast, critical information infrastructure focuses on the underlying information infrastructure, which consists of physical components and intangible information transmitted by and through those physical elements (ENISA, 2016). While acknowledging the conceptual overlap among critical infrastructure, critical information infrastructure, and national information infrastructure (Figure 1), this research prioritises cybersecurity and safeguarding critical information infrastructure in our rapidly evolving digital landscape.

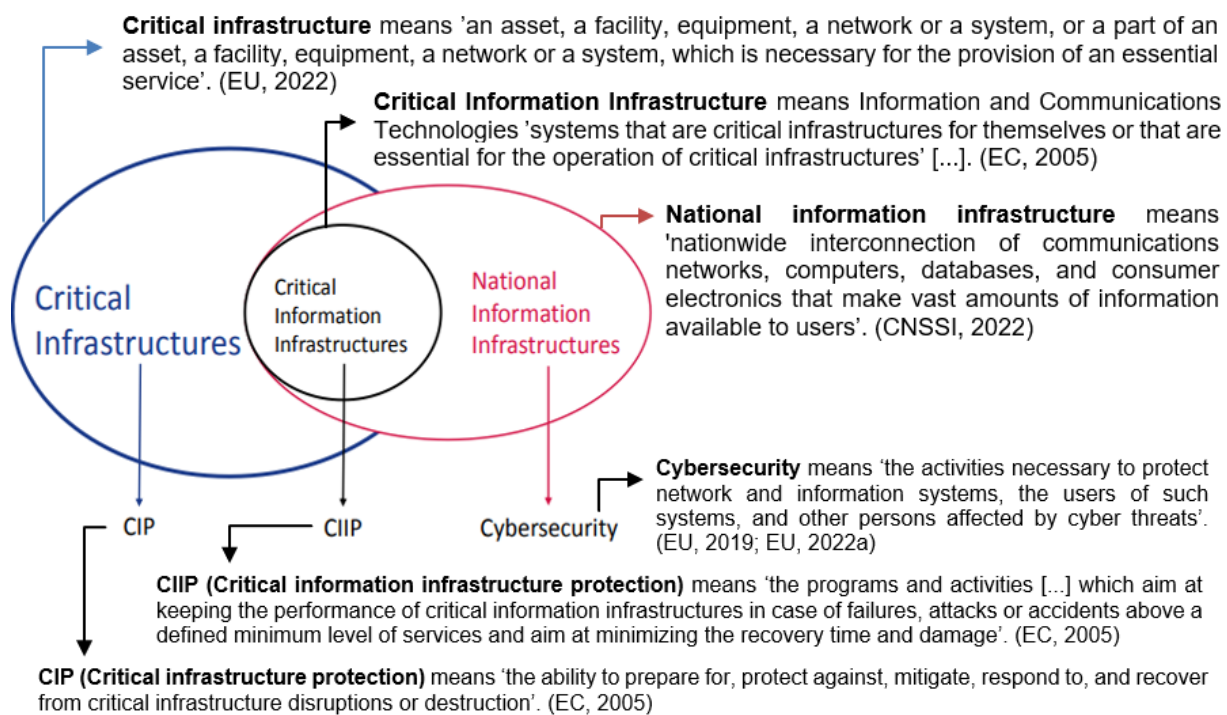


Figure 1. The interplay between critical infrastructures, critical information infrastructures and national information infrastructures. Source: Figure created by the author based on the European Union Agency for Cybersecurity figure (ENISA, 2016)

Safeguarding vital infrastructure is a shared objective among many nations. Still, the Lithuanian experience stands out due to its unique approach and how it solves this problem in line with other Baltic states. The distinctive Lithuanian perspective is characterised by a centralised framework that incorporates the domains of cybersecurity, the digital part of critical infrastructure protection, and critical information infrastructure protection, all falling under the competence of the Ministry of National Defence. While the predominant emphasis of this system revolves around cybersecurity, an initial phase involves precisely delineating and identifying the component elements of critical and information infrastructure. As a Lithuanian strategic approach, centralisation is pivotal in facilitating swift decision-making processes and ensuring better control over the domains above. However, in the complex context of critical infrastructure and critical information infrastructure, international legal instruments, such as the new EU Directive on the resilience of critical entities (CER Directive) (EU, 2022) and the new EU Directive on measures for a high common level of cybersecurity across the Union (EU, 2022a), introduce a nuanced perspective. These directives regulate critical infrastructure resilience, cybersecurity, and information infrastructure resilience from distinct legal grounds. In the Lithuanian context, this necessitates a reassessment of its current approach and practices with

the most recent provisions defined in the CER and the NIS2 Directives, which remain applicable until the 17th of October, 2024. By analysing Lithuania's specific challenges, we can draw broader lessons relevant to other nations facing similar concerns and focus on the unique context of protecting critical infrastructure as a national security interest.

The central thesis of this research paper asserts that Lithuania possesses the necessary mechanisms to adequately adopt and implement both the CER Directive and the NIS2 Directive. The research paper aims to understand whether Lithuania's legislative framework, conceptual documents, organisational architecture and practices meet EU requirements for safeguarding critical infrastructure. The research begins with an overview of Lithuania's legislative landscape and organisational structures related to critical infrastructure. It then dives into the provisions outlined in the CER Directive and the NIS2 Directive, considering Europe's goals and rationale for adopting them. It also analyses similarities and differences between the existing status quo in Lithuania and the requirements in these directives. Based on the literature review and the findings, this research provides a conclusion and recommendations for strategic leadership to improve the safety of critical infrastructure in the digital age.

1. Current critical infrastructure protection system in Lithuania

1.1. Legal Framework and Conceptual Documents

The first and most crucial step in formulating policies for the protection of critical infrastructure involves the integration of critical infrastructure protection within the framework of national legislation, accompanied by its adaptation to evolving international requirements. Lithuania's legal and regulatory frameworks provide the national model and policies for protecting critical infrastructure and maintaining national security. It is crucial for protecting critical infrastructure as it establishes a clear framework for governance, accountability, and enforcement (European Justice, 2023). Constitutional laws, ratified international treaties, and the Constitution are at the top of Lithuania's current legal and regulatory framework (European Justice, 2023). These foundational legal instruments establish the critical infrastructure's fundamental principles and obligations. As an EU Member State, Lithuania must harmonise EU regulations and directives into its national legal system, as they constitute an integral part of EU legislation (The European Parliament, 2023). Notably, the CER Directive

(focused on physical security) and the NIS2 Directive (focused on cybersecurity) are the latest EU directives about critical infrastructure protection (Figure 2). Within 21 months, Lithuania must incorporate these directives into its national legal framework by October 17, 2024 (EC, 2023). This process entails reviewing and adjusting existing systems, enhancing relevant frameworks, procedures, and operational practices and setting requirements for technical and organisational measures. The ultimate goal is to ensure full compliance with the CER and NIS2 Directive provisions, thereby bolstering the protection of essential services or infrastructure within the country. Detailed analysis of these requirements, Europe's rationale for adopting them, and a comparative assessment based on Lithuania's status will be explored further in subsequent chapters.

Below the top of Lithuania's current legal and regulatory framework are laws and legislative instruments, including resolutions from the Lithuanian Parliament and the Government. These provide global context and establish specific directives and standards (European Justice, 2023) for safeguarding critical infrastructure. Essential laws include the Law on the Basics of National Security (Seimas, 1996; Andžāns et al., 2021), which outlines Lithuania's fundamental framework for national security with a focus on strategically significant economic sectors. Additionally, the Law on the Protection of Objects of Importance to National Security (Seimas, 2002; Andžāns et al., 2021) identifies crucial objects for national security. It establishes a protective system for operators responsible for these objects and their transactions and investments, including critical information infrastructure. Furthermore, the Law on Crisis Management and Civil Protection (Seimas, 1998) delineates a comprehensive system for crisis prevention, preparedness, management, and mitigation of consequences arising from emergencies. Lastly, the Law on Cyber Security (Seimas, 2014) defines the critical information infrastructure protection system and prescribes regulations to enhance cybersecurity measures. These laws constitute the cornerstone of critical infrastructure and critical information infrastructure protection in Lithuania (Figure 2). The Law on the Management of State Information Resources (Seimas, 2011), which governs critical state information resources, will also be examined briefly in the final chapter.

The legislative resolutions by the Lithuanian Parliament and Government establish the imperative to protect and secure critical infrastructure, particularly critical information

infrastructure (Figure 2). The National Security Strategy (Seimas, 2021; Andžāns et al., 2021) provides the strategic framework for this protection, underscoring the importance of maintaining operational continuity of critical information infrastructure in crises by the highest cybersecurity and resilience standards—additionally, the strategy advocates for the use of equipment from trustworthy manufacturers. In support of the Cyber Security Law, the Government’s resolution (The Government of the Republic of Lithuania, 2018) endorses essential documents that form the basis of protection for critical infrastructure and critical information infrastructure: the Methodology for identifying critical infrastructure, Organizational and technical cybersecurity requirements along with the National cyber incident management plan, and the National Cyber Security Strategy (Figure 2). Beyond the documents above, various other legislative measures from ministries and government bodies set specific legal norms addressing critical information infrastructure protection. For instance, the Minister of National Defence’s order on the Typical plan for cyber incident management in essential information infrastructures (Minister of Defence, 2023) illustrates such regulatory efforts. The diagram below provides a schematic overview of Lithuania’s critical infrastructure structure, emphasising the existing primary legal and regulatory framework.

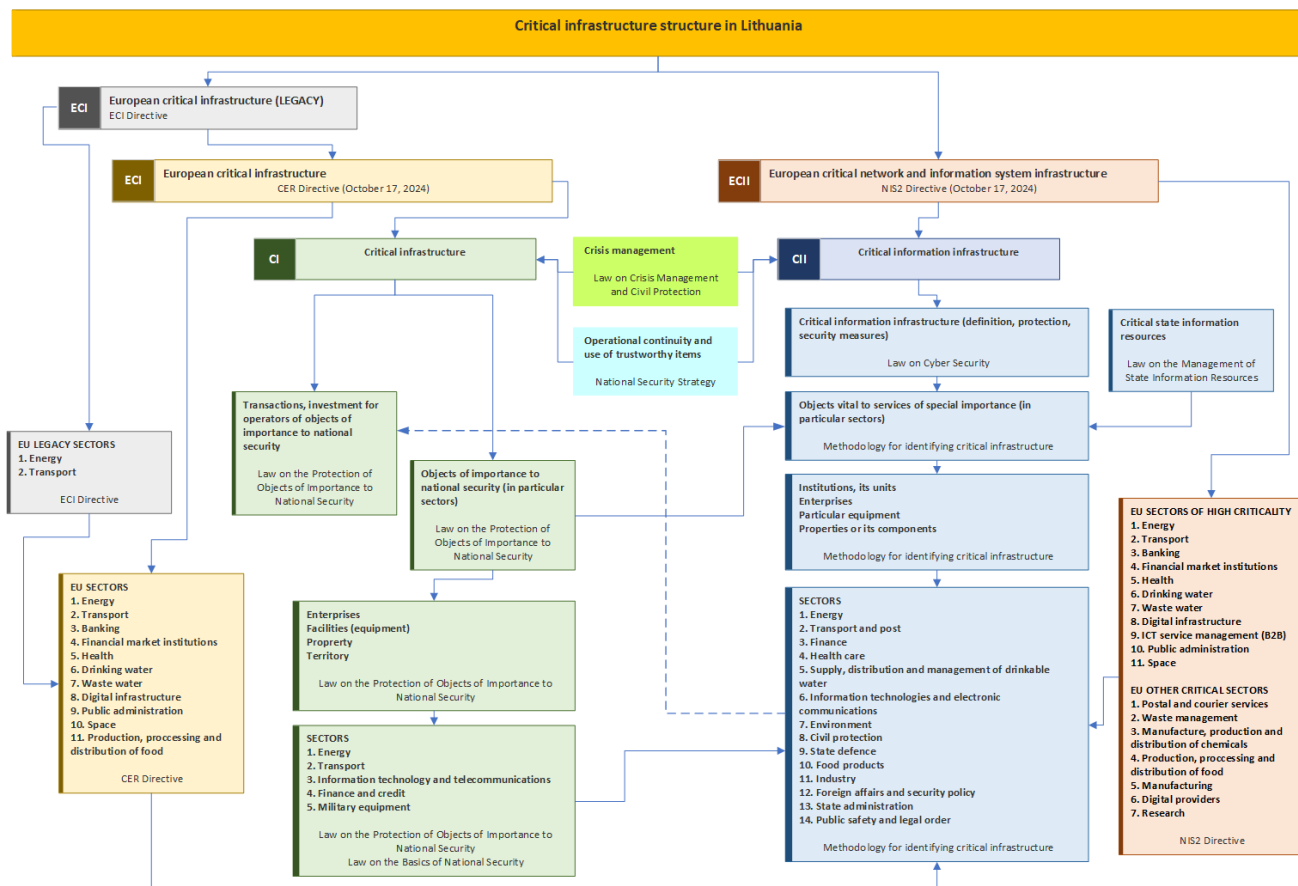


Figure 2. Critical infrastructure structure in Lithuania. Source: Figure created by the author based on Ramūnas Vilpišauskas figure (Andžāns et al., 2021)

As illustrated in Figure 2, Lithuania's existing critical infrastructure structure operates through several distinct yet closely interlinked regulatory layers. These layers play a pivotal role in safeguarding the nation's vital assets and ensuring national security. The layer positioned on the left-hand side of Figure 2 focuses on identifying and regulating objects of national security importance. It aims to shield enterprises, equipment, property, and territorial assets from risk factors that threaten national security. Within this layer, investment and transaction rules for enterprises are carefully governed, emphasising the need for robust protective measures. The layer on the right-hand side of Figure 2 directly addresses critical information infrastructure. It encompasses the design and allocation of protective measures and emphasises information infrastructure and cybersecurity. From a regulatory perspective, the diversity of legislative norms delineating the contours of critical infrastructure and prescribing its regulation structure gives rise to regulatory challenges concerning efficacy and practical implementation. A more optimal approach could involve the purification of legal norms by systematically applying cohesive criteria and collectively contributing to the robustness of the entire system.

In summary, Lithuania's multi-layered approach to protecting its critical infrastructure demonstrates a sophisticated understanding of the connections between its digital and physical assets. Although this system works, it has a complex regulatory environment that must be carefully managed because the layers have different origins and purposes. Some overlaps require continuous alignment as the legal framework develops (Figure 2). The harmonised regulatory framework for critical physical and digital infrastructure might be a more viable approach to navigate the complexities and ensure the resilience of national critical infrastructure, especially in small nations like Lithuania with limited resources.

1.2. Organizational Structures

The legal framework governing Lithuanian critical infrastructure significantly influences the national organisational architecture for critical infrastructure. Over time, legal changes have redefined functions, responsibilities, and competencies within the national institutional framework. This evolution shapes the current governance of

Lithuanian critical infrastructure, comprising several key components (Figure 3). The Lithuanian Parliament defines objects as being critical to national security, which qualifies as objects of critical infrastructure by the methodology for identifying critical information infrastructure (The Government of the Republic of Lithuania, 2018). Additionally, the Lithuanian Government legally identifies specific sectors and services as critical infrastructure and critical information infrastructure, forming a foundation of the existing system (Figure 3). The Ministry of National Defence serves as the central communication hub for the Government (The Government of the Republic of Lithuania, 2018) and oversees the approval process for compiling a list of critical infrastructure and critical information infrastructure assets, collaborates with other ministries and institutions to gather additional data and recommendations for assessing objects that may fall within the critical infrastructure category. It also communicates with the European Commission and orchestrates the exchange of information with other EU Member states in close collaboration with the National Cyber Security Centre, which operates under the Ministry of National Defence (Andžāns et al., 2021) (Figure 3). Next, the Government Commission plays a pivotal role at the national level (Seimas, 2002). As the central governing body, it holds authority over investment decisions, share transfers, equipment acquisitions, and system installations within enterprises critical to national security (Figure 3). Comprised of representatives from ministries and other institutions, the Commission assesses alignment with national security interests. Ultimately, the Government retains final decision-making authority, especially when transactions or investments conflict with national security (The Government of the Republic of Lithuania, 2009). The National Crisis Management Centre, operating within the Government, also enhances crisis preparedness and coordination (Seimas, 1998). This specialised entity serves as a central hub for managing and responding to crises and emergencies, proactively addressing critical infrastructure-related situations, and facilitating strategic communication concerning national security (Figure 3).

In governing critical information infrastructure, the Ministry of National Defence collaborates closely with the National Cyber Security Centre (Seimas, 2014; Andžāns et al., 2021) (Figure 3). Their joint efforts focus on assessing the alignment between information received by responsible institutions and the established Methodology for identifying critical information infrastructure (The Government of the Republic of Lithuania, 2018). The National Cyber Security Centre oversees quality control and methodological guidance during this evaluation. Following a thorough assessment, the

Ministry of National Defence compiles a list of preliminary critical information infrastructure objects and their operators and submits them to the Government for authorisation (The Government of the Republic of Lithuania, 2018; Andžāns et al., 2021). The National Cyber Security Centre is a central authority overseeing comprehensive cyber incident management, monitoring cybersecurity, ensuring compliance, and accrediting information resources (NKSC, 2024). The Cyber Security Council (Minister of Defence, 2015; Andžāns et al., 2021) facilitates discussions across public and private sectors to enhance cybersecurity assurance. This includes formulating proposals to refine the identification processes for specific critical infrastructure sectors and services deemed critical and information infrastructure and providing recommendations to operators managing critical information infrastructure (Figure 3). Ultimately, ministries and state institutions play a crucial role in identifying critical infrastructure and critical information infrastructure within specific sectors (Figure 3). These objects must meet specific criteria outlined in the Methodology for identifying critical information infrastructure (The Government of the Republic of Lithuania, 2018). As part of their participation in the system, each institution designates an individual responsible for critical infrastructure objects in critical sectors and information infrastructure identification. The contact details for these designated persons are submitted to the Ministry of National Defence. Responsible institutions will notify the included operators once the government approves the critical information infrastructure list. Furthermore, operators listed as critical must report any changes to the object or its operation to the responsible institution. Based on this reporting, the accountable institution conducts a review process for critical infrastructure identification or initiates a comprehensive review process for critical infrastructure identification in cases where no changes have been made over two years (Figure 3). The diagram below illustrates Lithuania's institutional framework for governing and overseeing critical infrastructure, critical information infrastructure, and critical infrastructure management.

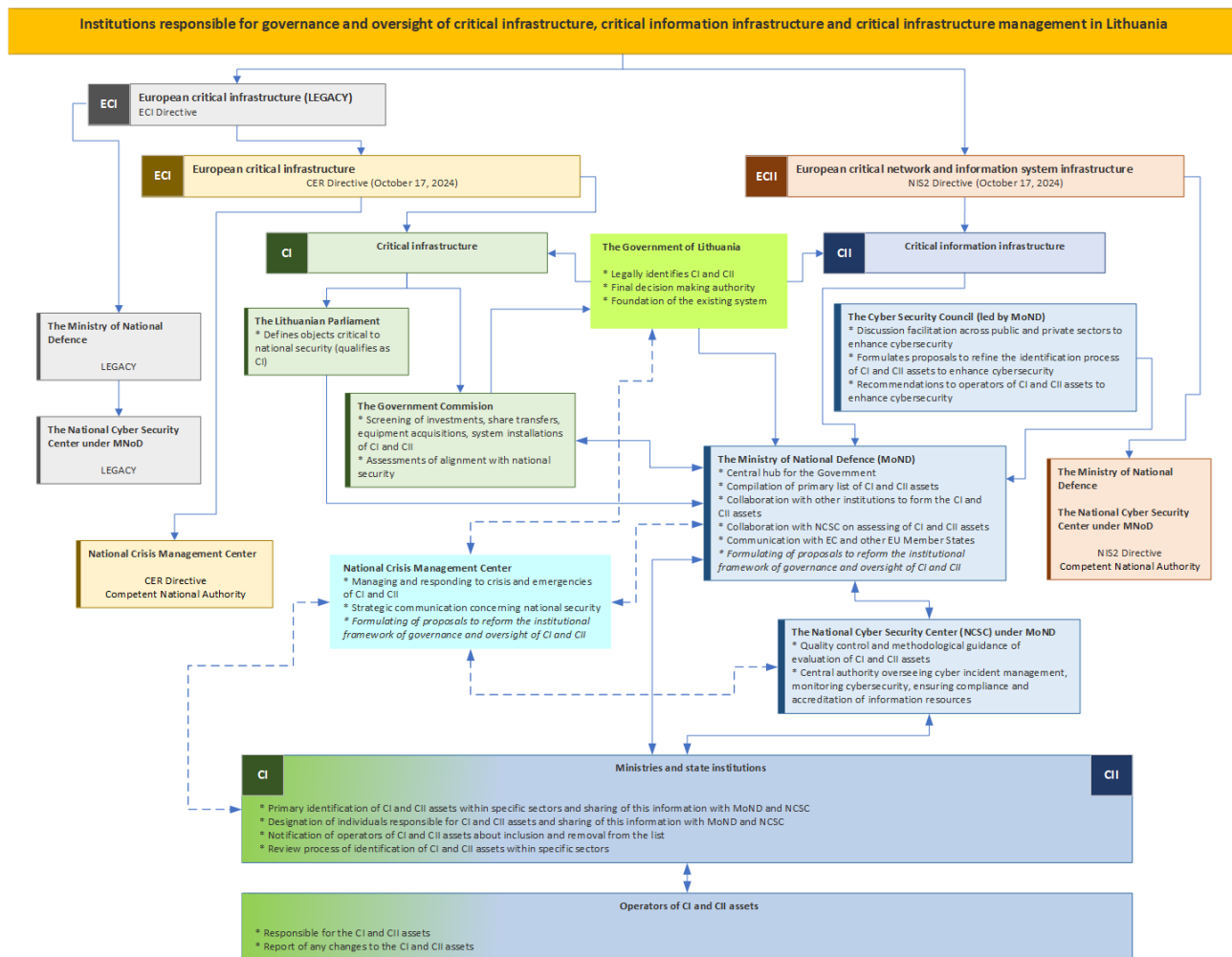


Figure 3. Institutions responsible for governance and oversight of critical infrastructure, critical information infrastructure and critical infrastructure management in Lithuania. Source: Figure created by the author based on Ramūnas Vilpišauskas figure (Andžāns et al., 2021)

Overall, the current organisational structure governing critical infrastructure in Lithuania has gradually improved within the legal framework and could be characterised as a structured approach and forms roles and responsibilities for all entities involved, ensuring governance and oversight of critical infrastructure and critical information infrastructure. Despite gradual progress in Lithuania’s critical infrastructure governance, several challenges persist. These challenges are laid down in the design of functions, responsibilities, and competencies within the national institutional framework. The presence of divergent hierarchical structures hinders complexity among entities responsible for overseeing critical and information infrastructure, resulting in different approaches that lack harmonisation. Notably, Lithuania’s critical infrastructure governance is presently experiencing a transitional phase. The National Crisis Management Centre and the Ministry of National Defence

are actively formulating proposals to reform the institutional framework responsible for the governance and oversight of critical infrastructure, critical information infrastructure, and its management. These proposed amendments align with the latest CER Directive and NIS2 Directive provisions, which all EU Member States, including Lithuania, must incorporate into their national legal framework by October 17, 2024. The success of this reform will depend on harmonising the legal framework governing the protection of critical and information infrastructure.

2. EU Critical Infrastructure Protection: Legislative Analysis and Strategic Outlook

2.1. Legislative Evolution: Motivations and Strategic Priorities

The evolving landscape of risks and limitations of previous legal frameworks has stimulated EU regulators to acknowledge the necessity for continuous regulatory enhancements as safeguarding critical infrastructure remains one of the central security priorities within the EU. In 2020, the European Commission introduced the EU Security Union Strategy from 2020 to 2025, focusing on priority areas where the EU can substantially support Member States in enhancing security for all residents of Europe (EC, 2020). One of these priority areas is creating a future-proof security environment, which includes cybersecurity and protecting critical infrastructure, that should be enhanced as the current framework for protecting and resiliency critical infrastructures has not kept up with the changing risks (EC, 2020a). To address existing weaknesses, the EU has replaced the outdated European Critical Infrastructure Directive (CEU, 2008) (ECI Directive) with the new CER Directive and the first common level of security for network and information systems (EU, 2016) (NIS1 Directive) with the NIS2 Directive. These legal initiatives aim to modernise critical infrastructure regulation and unlock its full potential, especially with the NIS2 Directive (Vandezande, 2024). Notably, the ECI Directive faced limitations due to the evolution of critical infrastructure governance through the last decade, divergent approaches among Member States in identifying potential critical infrastructures with subjective interpretations of what needed to be done by using different criteria for assessing risks, and insufficient data utilisation and missing systematic feedback and vulnerability assessment of critical infrastructure at the EU level (EC, 2019). The NIS1 Directive revealed significant challenges (Hristova-Ilieva, 2022), including inconsistencies and gaps arising from the de facto scope defined by Member States, which omitted critical

sectors. Additionally, divergent incident notification and security requirements across Member States, ineffective supervision, limited enforcement, and voluntary and ad-hoc cooperation and information sharing compounded the issues (Hristova-Ilieva, 2022). Moreover, implementing the NIS1 Directive demonstrated the need for Member States to enhance security and develop more effective protection measures (Contreras, 2023). After conducting a thorough stakeholder consultation, the European Commission determined that the NIS1 Directive needed to be revised due to several key issues, including the inadequate cyber resilience of EU-based businesses, the uneven resilience of different sectors and Member States, the lack of a shared understanding of the significant threats and challenges among Member States, and the absence of a coordinated crisis response (EC, 2020b). Furthermore, scholarly analyses posit that the NIS1 Directive lagged behind the mainstream recognition of cybersecurity as a critical policy area, extending into EU external relations and Common Foreign Security Policy (Carrapico & Barrinha, 2017).

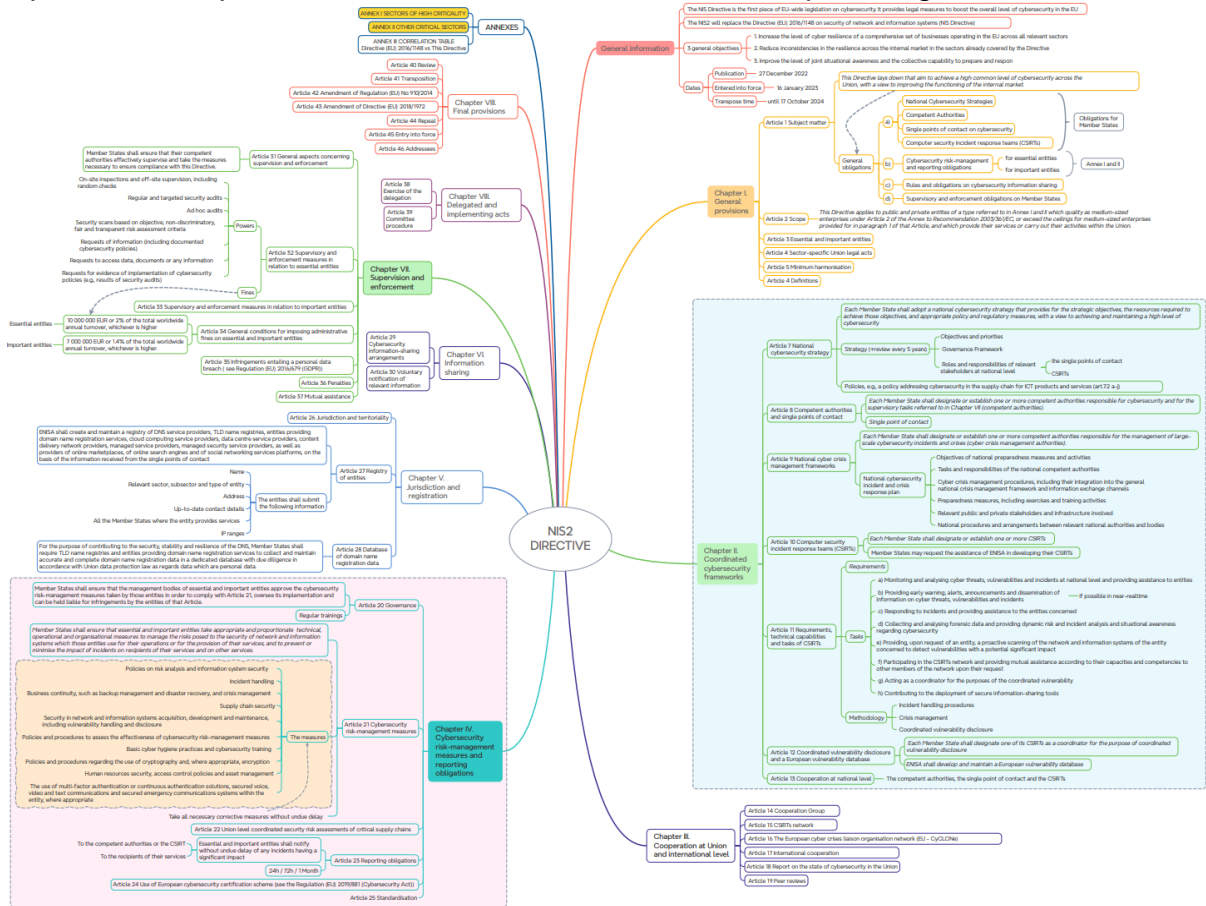
In light of these considerations, the EU needed to frame cybersecurity as a priority area, update the NIS1 Directive and ECI Directive to compete globally and maintain the EU legislative framework as a capable hub for critical infrastructure protection. The revision of EU directives governing critical infrastructure also represents a necessary and proactive measure to strengthen the EU's commitment to protecting its digital and physical assets in the rapidly changing threat landscape and the accelerating digitalisation of European society.

2.2. Member States' Obligations: Enhancing Resilience and Security

The EU's legislative framework for safeguarding critical infrastructure relies on two pivotal directives: the CER Directive and the NIS2 Directive. These directives establish minimum standards for Member States to enhance the resilience of essential sectors within the EU. The CER Directive primarily addresses the physical security of critical infrastructure, aiming to fortify its resilience against diverse threats, including terrorism, insider risks, sabotage, natural disasters, and public health emergencies (EC, 2024). In contrast, the NIS2 Directive focuses on cybersecurity and critical information infrastructure. It aims to enhance public and private entities' resilience, incident response capabilities, and competent authorities across the EU (EU, 2022a). Both documents are closely linked since the CER and NIS2 Directive were drafted simultaneously. Notably, entities designated as critical under the CER Directive fall under the regulatory framework of the NIS2 Directive (EU, 2022a), streamlining their application in cyberspace. Consequently, analysing the requirements of the NIS2 Directive takes precedence when safeguarding critical infrastructure in the digital realm.

The NIS2 Directive imposes mandatory obligations on Member States, covering several critical aspects (Figure 4). These obligations encompass defining terms and concepts, identifying organisations subject to the new regulations, and creating or revising national cybersecurity strategies (EU, 2022a). Additionally, Member States are empowered to establish competent authorities, cyber crisis management bodies, single points of contact dedicated to cybersecurity, and computer security incident response teams (CSIRT) (EU, 2022a). Furthermore, the NIS2 Directive advocates for robust governance requirements within regulated organisations to approve and supervise cybersecurity risk management measures and provide cybersecurity training (EU, 2022a). It also sets requirements for Member States to adopt appropriate technical, operational, and organisational safeguards that could effectively manage risks to network and information systems (EU, 2022a). The NIS2 Directive also emphasises the need in Member States to set requirements to manage third-party risks in supply chains and supplier relationships and to establish a layered approach for reporting cybersecurity incidents and other information sharing to the CSIRT or competent authority by specifying reporting criteria, the recipients of reports, and timelines for reporting (EU, 2022a). Additionally, the NIS2 Directive encourages establishing coordinated vulnerability disclosure practices, including reporting,

disclosing, and registering vulnerabilities in ICT products and services (EU, 2022a). Notably, the NIS2 Directive empowers designated competent authorities with comprehensive enforcement and investigative powers, including inspection, security audits, and requests for data, information, and documents (EU, 2022a). To ensure compliance, competent authorities are authorised to impose significant fines for



breaches of cyber security risk management and reporting obligations. Additionally, penalties can be enforced against management bodies of regulated organisations that fail to adhere to the provisions outlined in the NIS2 Directive (Figure 4).

Figure 4. NIS2 Directive obligations on Member States. Source: Figure created by the author based on Andrey Prozorov figure and NIS2 Directive (Prozorov, 2022; EU, 2022a) The EU's legislative framework for safeguarding critical infrastructure, specifically through the CER Directive and the NIS2 Directive, establishes comprehensive obligations for Member States. These directives aim to enhance the resilience of essential sectors within the EU by focusing on physical security and cybersecurity. These directives proactively reinforce the EU's commitment to safeguarding digital and physical assets in a rapidly changing threat landscape. Furthermore, the NIS2 directive is an essential step for the EU and its Member States to strengthen the implementation

of the CER Directive and improve the protection and resilience of their critical infrastructure in cyberspace.

3. Comparative Assessment of Lithuania's Cybersecurity Readiness

In previous chapters, we analysed Lithuania's legislative framework, conceptual documents, and organisational structures for critical infrastructure. We examined provisions from the CER Directive and the NIS2 Directive, considering Europe's rationale for adopting these directives and their intended outcomes. This chapter assesses Lithuania's preparedness for transposing these directives into its national legal framework. While specific data is still pending, our focus lies on comprehensively analysing the requirements outlined in the NIS2 Directive, particularly as it closely aligns with the implementation of the CER Directive when safeguarding critical infrastructure in cyberspace.

The initial focus of both directives centres around identifying entities subject to compliance requirements. In Lithuania, a methodology for identifying critical infrastructure exists, outlined in the Methodology for identifying critical infrastructure (The Government of the Republic of Lithuania, 2018). However, this process encounters several challenges. Firstly, integrating new sectors and additional criteria for identification into the regulated domain requires seamless assimilation. Secondly, transitioning from manual, paper-based identification to automation is essential because it needs more automation efficiency, and there is no centralised system where competent authorities can perform the identification process, nor do subjects have the means for self-identification. Thirdly, separating critical infrastructure and critical information infrastructure identification is necessary because the current approach predominantly focuses on safeguarding critical information infrastructure rather than addressing critical infrastructure objects. To address this, the National Crisis Management Centre could lead the critical infrastructure identification process, while the Ministry of National Defence could supervise the critical information infrastructure process. This division would ensure that each entity operates within its area of expertise. Lastly, the need for defined or specified dependencies between critical infrastructure sectors is slowing down coordination, resilience, and overall effectiveness in safeguarding critical infrastructure in Lithuania.

Another notable challenge Lithuania faces in complying with the NIS2 Directive is defining responsibilities and competencies among various authorities. Collaborative mechanisms must be established nationally, empowering these authorities through adequate supervision. Additionally, formulating sanctions for potential violations aligned with the NIS2 Directive is crucial. Lithuania operates under a fully centralised model, where joint efforts by the Ministry of National Defence and the National Cyber Security Centre constitute a single competent authority, a single point of contact dedicated to cybersecurity, and a single national CSIRT (EC, 2023a; Seimas, 2014; Andžāns et al., 2021). However, given the incorporation of additional sectors within the NIS2 Directive, it may be relevant to reconsider this model. Specifically, exploring multiple competent authorities and establishing additional CSIRTs, especially in the banking, ICT and other sectors, could enhance overall effectiveness. Furthermore, an institutional framework is needed to govern and oversee the national cyber crisis management system. As per existing legislation, the National Crisis Management Centre could be the primary operational entity responsible for cyber crises. Collaborating with the National Cyber Security Centre and the Ministry of National Defence would further strengthen the mission of the National Crisis Management Centre in this context.

Another noteworthy challenge to Lithuania's NIS2 Directive compliance is the issue of empowering designated authorities to advance cybersecurity practices. In Lithuania, existing frameworks facilitate on-site and off-site inspections, targeted security checks, and security audits conducted by competent authorities (Seimas, 2014; Minister of Defence, 2013). These evaluations assess the efficacy of cybersecurity risk management measures adopted by regulated entities, including evidence of the implementation of cybersecurity policies. However, opportunities for improvement exist. Leveraging competent authorities and auditors could strengthen the cybersecurity landscape across regulated sectors. To address this, an internal compliance audit could oversee the establishment of corrective measures. In contrast, an external audit by an independent body could ensure necessary corrective actions and provide essential oversight. Additionally, empowering competent authorities to perform objective security scans based on transparent risk assessment criteria would foster compliance. All these measures have the potential to enhance cybersecurity governance, foster compliance, and promote a more resilient and secure digital environment within regulated sectors. Regarding sanctions, Lithuania's administrative

code (Seimas, 2015) defines penalties for cybersecurity violations established by the Law on Cyber Security. However, these national sanctions lack effectiveness and proportionality compared to those outlined in the NIS2 Directive. While current Lithuanian fines are approximately up to 6 thousand EUR, the NIS2 Directive specifies penalties of up to 10 million EUR or at least 2 per cent of the total worldwide annual turnover for the previous financial year (whichever is greater) (EU, 2022a). Additionally, granting competent authorities the power to impose periodic fines on regulated entities for repetitive breaches would further enhance regulatory effectiveness.

In transposing the NIS2 Directive into national legal frameworks, a significant concern arises regarding the alignment of security requirements with the directive within domestic legislation. While the NIS2 Directive outlines desired objectives, it refrains from prescribing specific methods for achieving them. In Lithuania, the existing cybersecurity system is based on the NIS1 Directive. The primary regulatory framework for safeguarding critical infrastructure in cyberspace comprises the Law on Cyber Security (Seimas, 2014) and the Government's resolution (The Government of the Republic of Lithuania, 2018), which serves as the practical implementation mechanism for the former. Additionally, specific regulations governing critical infrastructure and its cybersecurity requirements are distributed across various laws, including the Law on the Protection of Objects of Importance to National Security (Seimas, 2002) and the Law on Electronic Communications (Seimas, 2004), which redirects essential sector-specific cybersecurity requirements to align with the overarching Law on Cyber Security. Furthermore, the Law on the Management of State Information Resources (Seimas, 2011) defines regulations for securing critical state information resources, including general electronic information security requirements (The Government of the Republic of Lithuania, 2013).

Despite the multifaceted legal landscape, implementing cybersecurity requirements across different sectors remains a complex challenge in Lithuania. No comprehensive solution exists for harmonising and revising cybersecurity requirements related to critical infrastructure. Several vital areas warrant attention to enhance the quality and effectiveness of critical infrastructure cybersecurity regulation. Firstly, consolidating requirements involves streamlining various cybersecurity mandates from different sectors into a unified set. This approach promotes clarity and consistency, enabling organisations to navigate the regulatory landscape more effectively. Secondly, the

granularity of security measures is crucial. Establishing a precise level of granularity ensures that security controls are appropriately tailored to the specific risks critical infrastructure faces. Factors such as asset criticality, threat vectors, and operational context could form the design of these measures. Thirdly, defining realistic timelines for implementation is essential. Balancing urgency with feasibility ensures effective compliance. Organisations must consider resource availability, complexity, and the need for phased adoption. Lastly, leveraging updated international standards enhances the robustness and interoperability of cybersecurity practices. Aligning with globally recognised frameworks enables critical infrastructure entities to leverage shared best practices and solutions. In the Lithuanian context, addressing these areas can strengthen the country's critical infrastructure cybersecurity regime, reduce administrative burdens, and enhance overall resilience against cyber threats. The NIS2 acknowledges the ISO/IEC 27000 series as a recognised standard (EU, 2022a). However, within Lithuania, the State Information Resources security requirements (The Government of the Republic of Lithuania, 2013) explicitly endorse this series of standards, although with an older version, necessitating an update to the latest iteration. The IEC 62443 set of standards emerges as a viable option for securing critical infrastructure operations. Furthermore, international standards can serve as primary guidance in implementing NIS2 requirements. Figure 4 illustrates the alignment of crucial NIS2 Directive requirements with these international standards.

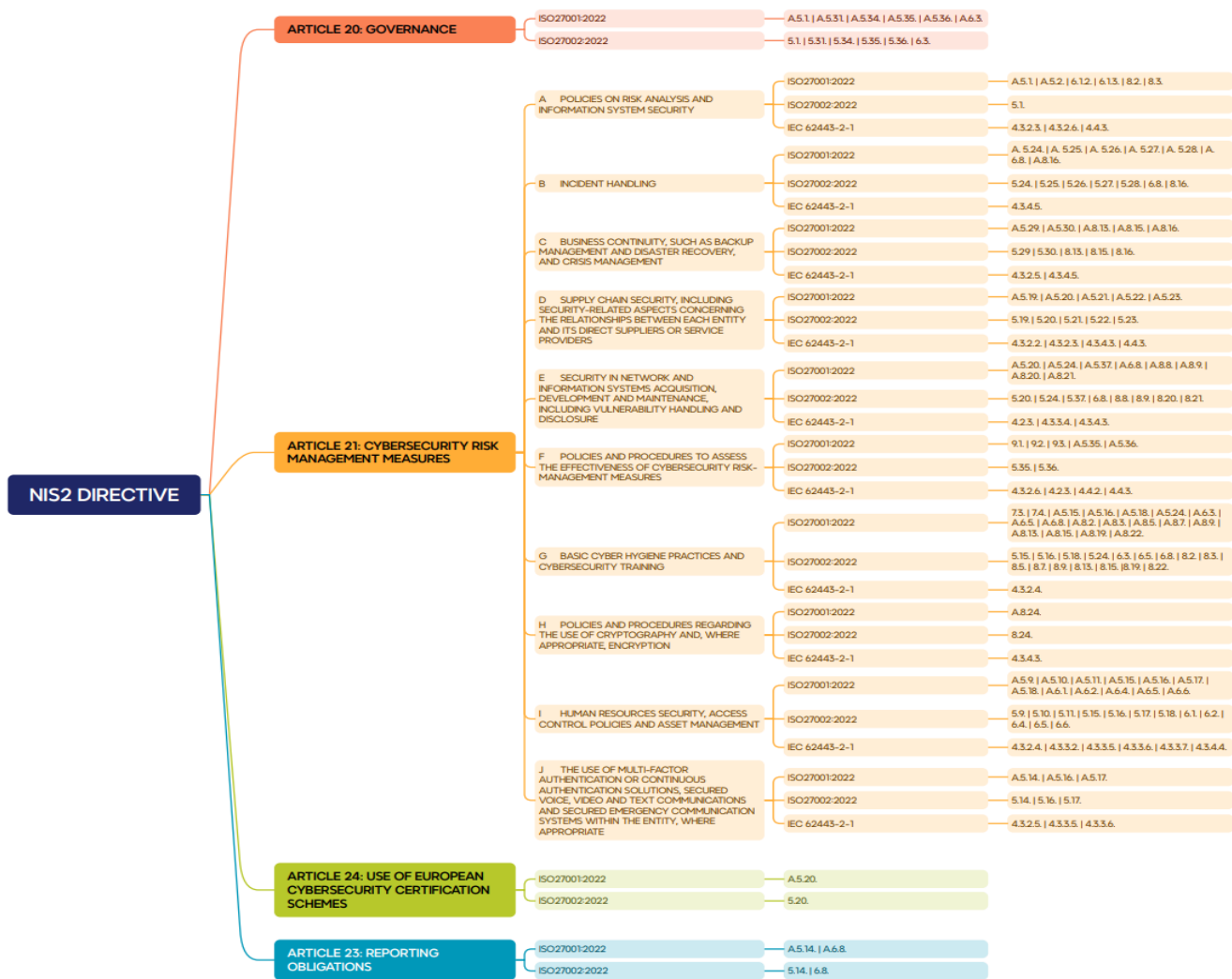


Figure 4. Mapping of crucial NIS2 Directive requirements with international standards. Source: Figure created by the author based on the ISO/IEC 27001:2022, ISO/IEC 27002:2022, and IEC 62443-2-1:2010 set of standards (ISO, 2022; ISO, 2022a; IEC, 2010)

In conclusion, Lithuania's adoption of the NIS2 Directive poses complex challenges for enhancing cybersecurity. These include integrating new sectors, automating identification processes, and establishing explicit dependencies among critical infrastructure sectors. Additionally, proper responsibilities, adequate supervision, and proportional sanctions are essential for compliance. The current centralised model of cybersecurity governance may require re-evaluation to accommodate the directive's expanded scope. Lastly, implementing security requirements aligned with the NIS2 Directive calls for consolidating sector-specific mandates, granularity of security measures, realistic timelines, and adopting updated international standards. Addressing these challenges will align Lithuania with the NIS2 Directive and fortify its digital environment against cyber threats.

Conclusion and recommendations

Lithuania has established a robust legal and organisational framework to protect its critical infrastructure, which is vital for national security. The centralised approach, led by the Ministry of National Defence, facilitates swift decision-making and precise control over cybersecurity, digital infrastructure, and critical information protection. However, the recent introduction of two significant EU directives (the CER Directive and the NIS2 Directive) presents Lithuania with the imperative task of reassessing its existing practices to align seamlessly with the latest provisions. The current centralised model of cybersecurity governance may necessitate re-evaluation to accommodate the expanded scope outlined in the directives. Other key challenges include integrating new sectors, automating identification processes, and establishing transparent interdependencies among critical infrastructure sectors. Furthermore, ensuring proper responsibilities, adequate supervision, and compliance sanctions remains a priority. Specifically, implementing security requirements aligned with the NIS2 Directive demands the consolidation of sector-specific mandates, granularity in security measures, realistic timelines, and adherence to updated international standards. Despite these challenges, Lithuania possesses the necessary mechanisms to adopt and implement EU directives effectively. Furthermore, its legislative framework and operational practices align with Europe's envisioned reality, ensuring sufficient critical infrastructure protection.

To enhance the protection of critical infrastructure in Lithuania, the following recommendations are proposed for strategic leadership, informed by the research findings:

1. Adjust and synchronise the implementation of both the CER Directive and NIS2 Directive into Lithuania's legal and regulatory frameworks to enhance the safeguarding of critical infrastructure in cyberspace.
2. Reinforce identifying critical infrastructure and critical information infrastructure processes, incorporating automation and self-identification capabilities and identifying dependencies among essential infrastructure sectors.
3. Review divergent hierarchical structures and establish clear responsibilities and competencies among authorities, ensuring adequate supervision and enforcement of cybersecurity measures with proportional and effective national sanctions.

4. Consolidate cybersecurity requirements into a unified set of regulations, align them with updated international standards, such as the ISO/IEC 27000 family, and periodically assess the effectiveness of these requirements to enhance cybersecurity governance and resilience.

By addressing these recommendations, Lithuania can better align with the EU's vision for cybersecurity and critical infrastructure protection, enhancing its resilience against evolving risks to critical infrastructure.

Bibliography

Andžāns, M., Sprūds, A., & Sverdrup, U. (Eds.). 2021. *Critical infrastructure in the Baltic states and Norway: strategies and practices of protection and communication*. Latvian Institute of International Affairs.

Carrapico, H., & Barrinha, A. 2017. The EU as a coherent (cyber) security actor?. *JCMS: journal of common market studies*, 55(6), 1254-1272.

CNSSI. 2022. No. 4009. *Committee on National Security Systems (CNSS) Glossary*. [Online] 2 March 2022. [Cited: 8 March 2024.] https://www.niap-ccevs.org/Ref/CNSSI_4009.pdf. *Committee on National Security Systems*

Contreras, P. 2023. The Transnational Dimension of Cybersecurity: The NIS Directive and Its Jurisdictional Challenges. In *Proceedings of the International Conference on Cybersecurity, Situational Awareness and Social Media: Cyber Science 2022; 20–21 June; Wales* (pp. 327-341). Singapore: Springer Nature Singapore.

ENISA. 2016. Stocktaking, Analysis and Recommendations on the protection of CIIs. *European Union Agency for Cybersecurity* [Online] 21 January 2016. [Cited: 28 February 2024.] <https://www.enisa.europa.eu/publications/stocktaking-analysis-and-recommendations-on-the-protection-of-ciis>.

European Justice. 2023. National legislation. Lithuania. *European e-Justice Portal* [Online] 7 April 2023. [Cited: 26 March 2024.] https://e-justice.europa.eu/6/EN/national_legislation?LITHUANIA&member=1.

IEC. 2010. *Industrial communication networks - Network and system security - Part 2-1: Establishing an industrial automation and control system security program* IEC 62443-2-1:2010. *International Electrotechnical Commission*

ISO. 2022. *Information security, cybersecurity and privacy protection — Information security management systems — Requirements* ISO/IEC 27001:2022. *International Organization for Standardization*

–. **2022a.** *Information security, cybersecurity and privacy protection — Information security controls* ISO/IEC 27002:2022. *International Organization for Standardization*

Hristova-Ilieva, B. 2022. Latest EU cybersecurity legislative initiatives– NIS 2 and CRA. *Presentation*. [Online] December 2022. [Cited: 8 March 2024.] <https://www.era.europa.eu/system/files/2022-12/01Policy-0%20-%20DG%20CNECT%20-%20Cyber%20Resilience%20Act%20and%20NIS2.pdf>.

Medeiros, B. P., & Goldoni, L. R. F. 2020. The fundamental conceptual trinity of cyberspace. *Contexto internacional*, 42, 31-54.

Minister of Defence, LTU. 2013. Dėl Nacionalinio kibernetinio saugumo centro prie Krašto apsaugos ministerijos nuostatų ir struktūros patvirtinimo. [Order on the approval of the provisions and structure of the National Cyber Security Center under the Ministry of National Defense]. *E-seimas*. [Online] 31 December 2013. [Cited: 2 April 2024.] <https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.463725/asr>.

–. **2015.** Dėl Kibernetinio saugumo tarybos reglamento ir personalinės sudėties patvirtinimo. [Order on the approval of the regulation and personnel composition of the Cyber Security Council]. *E-seimas*. [Online] 26 May 2015. [Cited: 6 April 2024.] <https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/543f8950046b11e5a0edd66091ee4d78/asr>.

–. **2023.** Dėl Tipinio kibernetinių incidentų valdymo ypatingos svarbos informacinėse infrastruktūrose plano patvirtinimo. [Order on the approval of the Typical plan for the management of cyber incidents in critical information infrastructures]. *E-seimas*. [Online] 16 October 2023. [Cited: 2 April 2024.] <https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/cbddab726c5b11eea182def3ac5c11d6?positionInSearchResults=0&searchModelUUID=b95cc445-ea54-4923-b05e-1c257bbbccbb>.

NSO. 2020. NATO Allied Joint Publication. AJP-3.20. Allied Joint Doctrine for Cyberspace Operations. Edition A Version 1. *NATO Standardization Office*

Pantin, N. T. 2017. *Key terrain: application to the layers of cyberspace* [Doctoral dissertation], Monterey, California: Naval Postgraduate School.

Porges, S. W. 2009. The polyvagal theory: New insights into adaptive reactions of the autonomic nervous system. *Cleveland Clinic Journal of Medicine*, 76 (Supl 2), S86.

Prozorov, A. [Facebook User]. 2022. NIS 2 mindmap [Online] 21 November 2022.

[Cited: 8 March 2024.]

<https://www.facebook.com/photo/?fbid=669693608184092&set=a.577352360751551>.

Seimas. 1996. *The Law on the Basics of National Security*. Vilnius, Lithuania: Seimas [Parliament of the Republic of Lithuania], 19 December 1996. Lietuvos Respublikos nacionalinio saugumo pagrindų įstatymas. VIII-49.

–. **1998.** *The Law on Crisis Management and Civil Protection*. Vilnius, Lithuania: Seimas [Parliament of the Republic of Lithuania], 15 December 1998. Lietuvos Respublikos krizių valdymo ir civilinės saugos įstatymas. VIII-971.

–. **2002.** *The Law on the Protection of Objects of Importance to National Security*. Vilnius, Lithuania: Seimas [Parliament of the Republic of Lithuania], 10 October 2002. Lietuvos Respublikos nacionaliniam saugumui užtikrinti svarbių objektų apsaugos įstatymas. IX-1132.

–. **2004.** *The Law on Electronic Communications*. Vilnius, Lithuania: Seimas [Parliament of the Republic of Lithuania], 15 April 2004. Lietuvos Respublikos elektroninių ryšių įstatymas. IX-2135.

–. **2011.** *The Law on the Management of State Information Resources*. Vilnius, Lithuania: Seimas [Parliament of the Republic of Lithuania], 15 December 2011. Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas. XI-1807.

–. **2014.** *The Law on Cyber Security*. Vilnius, Lithuania: Seimas [Parliament of the Republic of Lithuania], 11 December 2014. Lietuvos Respublikos kibernetinio saugumo įstatymas. XII-1428.

–. **2015.** *Law on Procedures for the Approval, Entry into Force, and Implementation of the Code of Administrative Offenses*. Vilnius, Lithuania: Seimas [Parliament of the Republic of Lithuania], 25 June 2015. Lietuvos Respublikos administracinių nusižengimų kodekso patvirtinimo, įsigaliojimo ir įgyvendinimo tvarkos įstatymas. XII-1869.

–. **2021.** Resolution on the Approval of the National Security Strategy. *Lietuvos Respublikos Seimas*. [Online] 16 December 2021. [Cited: 4 April 2024.] <https://www.e-tar.lt/portal/legalAct.html?documentId=f54863b0623a11eca9ac839120d251c4>.

The Council of the European Union (CEU). 2008. Council Directive 2008/114/EC. *Eur-lex*. [Online] 8 December 2008. [Cited: 7 March 2024.] <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32008L0114>.

The European Commission (EC). 2005. Green Paper on a European programme for critical infrastructure protection. *Eur-lex*. [Online] 17 November 2005. [Cited: 8 March 2024.] <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52005DC0576>.

–. **2019.** Evaluation study of Council Directive 2008/114 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection – Final report. *Directorate-General for Migration and Home Affairs*

–. **2020.** The EU Security Union Strategy. *The European Commission* [Online] 11 September 2020. [Cited: 7 March 2024.] <https://ec.europa.eu/newsroom/pps/items/686851/>.

–. **2020a.** Communication from the Commission on the EU Security Union Strategy. *Eur-lex*. [Online] 24 July 2020. [Cited: 7 March 2024.] <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0605>.

–. **2020b.** New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient - Questions and Answers. *The European Commission* [Online] 16 December 2020. [Cited: 24 March 2024.] https://ec.europa.eu/commission/presscorner/api/files/document/print/en/qanda_20_2392/QANDA_20_2392_EN.pdf.

–. **2023.** New stronger rules start to apply for the cyber and physical resilience of critical entities and networks. *The European Commission* [Online] 16 January 2023. [Cited: 26 March 2024.] <https://digital-strategy.ec.europa.eu/en/news/new-stronger-rules-start-apply-cyber-and-physical-resilience-critical-entities-and-networks#:~:text=Member%20States%20have%2021%20months%20to%20transpose%20both,publish%20the%20measures%20necessary%20to%20comply%20with%20them..>

–. **2023a.** Implementation of the NIS Directive in Lithuania. *The European Commission* [Online] 23 February 2023. [Cited: 8 March 2024.] <https://digital-strategy.ec.europa.eu/en/policies/nis-directive-lithuania>.

–. **2024.** Critical infrastructure resilience. *The European Commission* [Online] 21 March 2024. [Cited: 24 March 2024.] https://home-affairs.ec.europa.eu/policies/internal-security/counter-terrorism-and-radicalisation/protection/critical-infrastructure-resilience_en.

The European Parliament and the Council of the European Union (EU). 2016. Directive (EU) 2016/1148 of the European Parliament and of the Council. *Eur-lex*. [Online] 6 July 2016. [Cited: 7 March 2024.] <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32016L1148>.

–. **2019.** Regulation (EU) 2019/881 of the European Parliament and of the Council. *Eur-lex*. [Online] 17 April 2019. [Cited: 8 March 2024.] <https://eur-lex.europa.eu/eli/reg/2019/881/oj>.

–. **2022.** Directive (EU) 2022/2557 of the European Parliament and of the Council. *Eur-lex*. [Online] 14 December 2022. [Cited: 8 March 2024.] <https://eur-lex.europa.eu/eli/dir/2022/2557/oj>.

–. **2022a.** Directive (EU) 2022/2555 of the European Parliament and of the Council. *Eur-lex*. [Online] 14 December 2022. [Cited: 8 March 2024.] <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32022L2555>.

The European Parliament. 2023. Sources and scope of European Union law. *The European Parliament*. [Online] November 2023. [Cited: 26 March 2024.] <https://www.europarl.europa.eu/factsheets/en/sheet/6/euopos-sajungos-teises-saltiniai-ir-taikymo-sritis>.

The Government of the Republic of Lithuania. 2009. Resolution on the approval of the work procedure description of the coordination commission for the protection of objects important for ensuring national security. *Lietuvos Respublikos Seimas*. [Online] 25 November 2009. [Cited: 2 April 2024.] <https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.359678/asr>.

–. **2013.** Resolution on the approval of the description of the general requirements for the security of electronic information and the description of the guidelines for the content of security documents. *Lietuvos Respublikos Seimas*. [Online] 24 July 2013. [Cited: 2 April 2024.] <https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.454399/asr>.

–. **2018.** Resolution on the Approval of the National Cyber Security Strategy. *Lietuvos Respublikos Seimas*. [Online] 13 August 2018. [Cited: 4 April 2024.] <https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/94365031a53411e8aa33fe8f0fea665f/asr>.

NKSC. 2024. About National Cyber Security Centre. *The National Cyber Security Centre* [Online] 2024. [Cited: 6 April 2024.] <https://www.nksc.lt/veikla.html>.

Vandezande, N. 2024. Cybersecurity in the EU: How the NIS2-directive stacks up against its predecessor. *Computer Law & Security Review*, 52, 105890.

LIIVI TURK. What should be a successful strategy for a small state. Example of Estonia.

Introduction

*The strong do what they have the power to do,
and the weak accept what they must accept.*

(Thucydides 431, B.C.E.)

*So David triumphed over the Philistine with a sling and a stone;
without a sword in his hand, he struck down the Philistine and killed him.*

(1 Samuel 17:41-52)

With the adoption of the North Atlantic Treaty Organisation (NATO) Strategic Concept in 2022, NATO allies agreed on the understanding that ‘during the last decade, the world has radically changed to more unstable, with growing strategic competition, pervasive instability and recurrent shocks defining the broader security environment for the transatlantic, value-based societies’ (NATO, 2022). The developments in the world since then are adding to the concerns: the war in Ukraine is ongoing, in October 2023, the Israel-Palestinian violent conflict broke out, and international shipping is threatened in the Red Sea by the Houthi rebels, to name the most visible military-political concerns.

Estonia is a small NATO ally and European Union (EU) member state situated geographically in a perfect four-season location, but unfortunately, it is too small to guarantee its security independently in its geopolitical location as a neighbour of the Russian Federation (Russia). The outlook of the security environment for Estonia, according to the Estonian National Risk Analysis 2023, is troubling, drawing from the military aggression of Russia against Ukraine the conclusion that war in Europe is not unthinkable, and Estonia must prepare to protect its sovereignty and its people and be ready to mobilise all available resources (Riigikantselei, 2023). Estonian national security and defence documents have echoed similar challenges for years, highlighting that the competition has become an open confrontation (National Security Concept

2023, also in NDPP 2021, EFIS, 2024). Similar concerns are present in NATO and EU strategic documents (ACT, 2023; NATO, 2022). In addition, there have been several statements from politicians of different states about the possibility of aggression or testing of NATO, whereas the beginning of the possible war varies from three to twenty years (RUSI, 2024).

To be better prepared for the future, both NATO and the EU also look for ways for necessary developments to be better prepared. In NATO, there is a dedicated Warfighting Capstone Concept, offering a vision to support the maintenance and further development of NATO's military power. It foresees that adaption to future challenges requires the allies to concentrate on focused exploitation of data and technology, agility to develop capabilities, the right people with the right skills, and persistent preparation of all military capabilities as well as integration with other actors and instruments of power (ACT, 2021). In the EU, there is a clear understanding of increasing the defence expenditures to address the urgent procurement needs, overcome the capability gaps and enhance the European Defence Technological and Industrial Base (EDTIB) across the board. In addition, several steps have been taken to increase the capacity for innovation and disruptive technologies and reduce strategic dependencies (EUEA, 2024). The ongoing war in Ukraine has confirmed the importance of innovation, be it the wide use of drones or the environment that encourages bottom-up innovation by young officers (Jones et al., 2023; Franke, 2023; Pettyjohn, 2024).

Taking these developments in the security situation and the predictions that the coming years will most likely bring even more competition, developments, and complexity, it is essential to review what the strategy for Estonia should be. The underlying thesis of this paper is that Estonia has the potential to create a niche capability in innovation, both to be better prepared for future challenges and to offer added value to its allies and partners.

This research paper has six parts. The first is an overview of strategy-making, focusing on strategies for small states. The second part analyses the main goals and elements in Estonian strategic documents, looking for possibilities to establish itself a niche capability. The third looks at the Estonian current achievements in potential areas for niche capability. The fourth draws an overview of the developments in the field of

innovation in NATO and the EU with the fifth part giving an overview of the developments in the field of defence innovation in Estonia, including recommendations for the future. In the conclusion, the main findings will be presented.

Strategy as the formula for achieving the goals

There is an abundance of literature on strategy, the evolution of the idea, its use in different areas, the great strategy of great powers and slightly less about the strategy of smaller states. There are also voices claiming that the strategy is dead, both because of the proliferation of the use of strategy away from its traditional meaning and connection to the military and war (Strachan, 2006). The rise of the speed of changes, especially in the field of technology and digitalisation, has added another element to this, arguing that strategic positioning is not valid anymore, and there is a need for continuous innovation and agility (Strebel, 2017).

Accepting the need for agility and innovation, the current paper finds forward-looking strategic thinking necessary. It is based on the understanding that 'strategy, although an imprecise art, is irreplaceable, directing the actions to achieve the goals in the contested environment' (Brands, 2023, p 1-11). Moreover, taking the current volatile security situation, the importance of strategy is even greater – 'strategy is most valuable when the stakes are high, and the consequences of failure are severe' (Brands, 2023, p 1). In the scope of this paper, three main elements of the strategy are highlighted – grand strategy, the ideal formulation of the strategy and strategy for the small states.

Grand strategy can be defined as focusing only on the most significant interests a nation seeks to advance or defend and not with all long-term foreign policy goals. States develop a grand strategy for practical reasons. Formulating the strategy helps leaders clarify their thinking about the state's role in the world and guiding the whole of government (RAND, 2021). Nina Silove argues in her article, offering a comprehensive overview of the evolution of the term grand strategy, that there is no agreed or authoritative definition (Silove, 2018). The idea of strategy was developed and applied by military historians to mean the deliberate strategy employed by officials to win a war and create the conditions for future peace, drawing from among all the state's resources. The essential elements of different scientific approaches to the strategy are

the ends, ways and means, long-termism (for decades or even centuries) and holistic approach, encompassing all the state resources.

Grand strategies are generally used in connection with the great powers, as the great powers have far more significant effects on important outcomes in the international system than smaller states. At the same time, small states can also have grand strategies, choosing what ends to prioritise, how to use the resources, and what means to devote to these ends. It is also important to note Silove's finding that although the basis of the literature on the grand strategy shares the assumption that there is a positive correlation between having the strategy and the positive impact, it still needs to be clearly articulated and empirically examined. The often-cited quote by D.D. Eisenhower can support this argument. Eisenhower said that a plan is nothing; planning is everything, referring thus to the importance of planning and accepting that reality can not go according to the plan.

Content-wise, the strategy is most usually defined as the ends-ways-means formula, using the means in the best ways to reach the desired ends. However, there are also arguments that it can lead to a strategy that is uncreative, noncritical, and limiting new and adaptive thinking (Meiser, 2016). The ideas on how to overcome this challenge are to ensure that the assumptions are probed and checked (Brands, 2023, 12) or adopt different thinking, such as 'defining strategy as a theory of success and understanding that the purpose of strategy is to create advantage, generate new sources of power, and exploit weaknesses in the opponent' (Meiser, 2016). The benefit of such an approach is that the strategy will become an explanation of how obstacles can be overcome, creating opportunities, magnifying existing resources, or creating new resources rather than staying too rigidly within the limits of the existing means and ways. In the current volatile security situation, the latter approach seems to be getting growing attention, combined with strategic leaders' need for creative thinking (Carr, 2024).

When it comes to the strategies of the small states, their smallness inevitably sets certain limits to their strategies and strategic goals. There are different approaches to how to define smallness. Based on the comprehensive study by Baldur Thorhallsson of the literature overview encompassing the small states, the following main aspects of defining small states can be drawn out: population size being the most popular (below 10 or 15 million, or less), economy, territory, small military (Thorhallsson, 2018; see also Dyčka, 2020). Thorhallsson argues that as the small size of the population

and economy limits the resources available to the state, then the grand strategy of the small state must be understood as rather than being a theory of victory, 'a theory of avoiding defeat or destruction' (Thorhallsson, 2018).

As a remark, it is important to note that after the II World War, there was considerable change towards introducing international norms to the direction of avoiding war, the establishment of the United Nations (1945), the European Union (the first development from 1948), OSCE (1975) for example. Such developments have made the world a much safer place for the states that cannot afford the capabilities to protect themselves militarily from stronger states, and in addition, the consensus-based decision-making has also given remarkably stronger diplomatic power to the small states (see Wivel, 2021; Väyrynen, 1997) as well as offering a forum to deliver the positions. However, these changes have not made the states equal players in international relations, especially when it comes to guaranteeing the security of the states, and the small states still need to look at how to improve or overcome their smallness.

Traditionally, and according to the overview by Wivel, the solutions for small states' security have been shelter-seeking and hiding, whereas shelter-seeking means cooperation with great power, and hiding stands for neutrality. The concept of shelter-seeking in his overview as being connected to great power can be extended to membership in alliances, especially to NATO. It has been a case for Estonia (Praks, 2019) and can also be attributed to the case of Finnish and Swedish accession to NATO after Russia's full-scale invasion of Ukraine. At the same time, since shelter-seeking means depending on the great power, the small state also faces a risk of abandonment by stronger allies if it signals a weak commitment to alliance obligations or fails to support other alliance members in specific conflicts. That becomes especially frightening considering Donald Trump's public opinion on the allies that are not fulfilling the 2% commitment to NATO (The Guardian, 2024).

According to Wivel, the usual reason for the small states' successful strategy is an inclination to innovative, nimble and flexible responses to globalisation. Besides flexibility, an important factor of a successful small-state strategy is its strength in some niche capability, which could also be political discourse and the self-perception of the political leader (Wivel, 2021; see also Thorallsson, 2018; Dyčka, 2020).

To sum up, according to the literature, a successful small-state grand strategy is either shelter-seeking or hiding and ideally also includes a niche capability. The next

paragraph will analyse the main goals of the current Estonian strategic documents and the potential areas for developing a niche capability.

The main elements in the current strategic documents

There are two guiding principles of the Estonian security and defence policy, having its roots in the loss of independence by the Soviet occupation in 1940: 1) “Estonia will fight back” and 2) “never alone again” (Praks, 2019). The principle “never alone again” reflects well that according to the previous overview of the literature on the strategies of small states, Estonia has firmly chosen a shelter-seeking approach, especially in the form of membership in international (defence) organisations and alliances. Both principles are firmly embedded in official documents directing and driving Estonian development. These are the strategies for Estonia 2035 (Estonia 2035, 2023), National Security Concept 2023 (National Security, 2023), and National Defence Development Plan 2031 (National Defence, 2023). In the current strategy documents, the main emphasis seems to be on the broad need to safeguard the security of Estonia with multiple actions and aspects, and the inclination to develop a specific niche capability can only vaguely be deducted.

According to the long-term strategy of Estonia 2035, Estonia in 2035 should be an innovative country of smart people with a strong international position, highly reliable cyberspace, and an innovative and knowledge-based economy using new technologies. The National Security Concept foresees the Estonian economy focusing on innovative technological solutions and emerging technologies, whereas the military defence is based on solid defence resolve, deterrence by denial, combining both Estonian individual capabilities with the combat-ready Allied forces.

The National Defence Development plan strongly emphasises building societal resilience, security of supplies and communications and the cyber sphere. As a more specific element under international cooperation, the development of cyber diplomacy and cyber defence as important aspects is mentioned. In military defence, the main elements are building the conventional capabilities, such as expanding the wartime structure, increasing the protection of units, strengthening the anti-tank capabilities of units and the 2nd Infantry Brigade's self-propelled artillery, and improving the intelligence and situational awareness capabilities. As the plan was renewed in 2023, new developments, such as a multiple rocket launcher unit with regional range

capability and enhancing coastal defence with anti-ship missiles and mines, were added.

The main keywords that emerge as repetitive from the Estonian strategic documents that could be potentially seen as the elements to establish niche capabilities are the following: international solid position, cyber, and innovation (in the broadest meaning, including both technology and innovative people). The following paragraph will see what Estonia has done to implement these elements.

Implementing the elements of potential niche capabilities

Estonia's strong position in the international arena has emerged, especially after the start of Ukraine's full-scale aggression against Ukraine. The war revealed Russia's aggressiveness and confirmed its readiness to use military force to achieve foreign policy goals. Estonia started to be one of the most vocal in the international arena in preaching the need to support Ukraine and restrict Russia internationally, including suggesting a military strategy for Ukraine's victory (MoD, 2023a), to name the most prominent. Estonia also led Ukraine by example, being the highest per capita contributor (Kiel Institute, 2024). Such leadership brought Estonian Prime Minister Kaja Kallas to the spotlight. It earned her the name of Estonian Iron Lady (Newstatesman, 2024), a position in the Times 100 Most Influential Leaders in 2022 (Time, 2022) and eventually (and in-directly) also caused blacklisting by Russia (AP News, 2024).

Regarding cyber, Estonia is one of the most digitalised countries, where most public services are available online (E-Estonia, 2024). Together with building digital services, Estonia has put much effort into cybersecurity, especially after the cyberattacks in 2007, which has made Estonia known as a leading speaker for cybersecurity and fostering innovation in defence against cyber threats (Wivel, 2021, also Bhatti, 2024). There have been several positive developments in the defence field, such as the establishment of the NATO Cooperative Cyber Defence Centre of Excellence in Tallinn and the establishment of Cyber Command and Cyber Defence Unit in the Estonian voluntary Defence League.

The digital solid infrastructure also supports Estonia's positioning in 16th place in innovation in the global context, showing high cores at infrastructure and market sophistication (Global Innovation, 2023); at the same time, in the European context,

Estonia scores as a moderate innovator, with the strengths at trademark applications, lifelong learning, scientific publications, and employment in innovative enterprises. The weaknesses, however, are, among others, resource productivity, government support for business research and development and medium and high-tech goods exports (European Innovation, 2023).

Regarding innovation, especially in the defence field, the Estonian National Defence Development Plan's focus on military capabilities is on conventional capabilities and less on innovation and new technologies. Considering the military reforms declared by Russian Defence Minister Shoigu on 21 December 2022 (RFERL, 2021), which will increase Russian military strength behind the NATO border considerably, it is understood and well-founded and also connected with Article 3 in the NATO Treaty, stating the need of allies to develop the individual capacity to resist armed attack. The need for robust conventional capabilities is evident also in the ongoing war in Ukraine.

However, the war in Ukraine also shows the impact that new technologies, such as drones, software-defined warfare, artificial intelligence, and space technology, have (Franke, 2023). In addition to the use of technology and good civil-military cooperation, Ukraine's experience highlights the importance of innovative thinking among the officers (Jones et al., 2023) and the benefit of education in science, technology, engineering, and mathematics (STEM) (Muravska, 2023). Therefore, by acknowledging the importance of innovation in the defence field and implementing these elements to the extent possible, Estonia could create itself a niche capability and a strength that would be useful also to allies.

Recent developments in the field of innovation in NATO and the EU

The literature on defence innovation distinguishes defence innovation from military innovation. According to Mahnken, Ross, and Cheung's definition, defence innovation is a broader term for 'transforming ideas and knowledge into new or improved products, processes, and services for military and dual-use applications' (Cheung, 2021). In contrast, military innovation is seen as placing 'more emphasis on doctrinal and warfighting issues' (ibid) and further elaborated as both the outcome and the process of three layers: invention, incubation and implementation, all designed to enhance the ability to generate power and leading to change in conducting warfare (Horowitz, 2023).

Innovation as a new area changed the environment, and warfighting for NATO is stated in the NATO ACT foresight looking into the world in 2024. It states that AI and emerging and disruptive technologies (EDTs) 'will reshape states, societies and armed forces as well as the character of competition and warfare with unprecedented speed' (ACT 2023). Promoting innovation also has a clear role in the latest NATO Strategic Concept 2022, emphasising the importance of investing in innovation (NATO, 2022).

To support NATO allies in innovation, NATO established the NATO Innovation Fund (NIF) in 2023, with Estonia among the founding members. The fund aims to be the 'first multi-sovereign venture capital fund, stimulating the trans-Atlantic deep tech landscape' (NIF, 2023). In addition to NIF, the Defence Innovation Accelerator for the North Atlantic (DIANA) was established, providing companies with the resources, networks, and guidance to develop dual-use deep technologies that contribute to defence (DIANA, 2022), whereas Estonia, together with the UK was chosen to create the DIANA European headquarters (MoD, 2022). In addition, NATO has already 2021 adopted a strategy for emerging and disruptive technologies, later artificial intelligence, and created boards for implementing the principles and monitoring the developments in the area, such as the NATO Advisory Group on Emerging and Disruptive Technologies, NATO's Data and Artificial Intelligence Review Board, NATO Innovation Board¹⁰, all offering opportunities also for Estonian participation.

A similar approach can be found in the EU. The EU Strategic Compass explains the strategic environment with the adversaries using emerging and disruptive technologies to seize strategic advantages. It, therefore, foresees as one main line of efforts investing to 'jointly develop cutting-edge military capabilities and invest in technological innovation for defence and create a new Defence Innovation Hub within the European Defence Agency' (Council of, 2022). As a result, the Hub for EU Defence Innovation (HEDI) was established in 2022 based on EDA's existing Innovation Framework, aiming to foster innovative solutions for defence and increase cooperation on defence innovation among Member States (EDA, 2022). As a tool to support research and development, the European Defence Fund (EDF) was created already in 2020, with allocated funds of 8 billion for 2021-2027 to encourage collaboration in the field of research and development. In the recently adopted European Defence Industrial

¹⁰ Overview of NATO innovation activities: https://www.nato.int/cps/en/natohq/topics_184303.htm

Strategy, innovation is essential in achieving defence readiness and strengthening EDIDP (New Strategy, 2024).

The possibilities for Estonia to create niche capability in innovation

Regarding defence innovation in Estonia, several developments have been made. Already in 2009, the predecessor of the current Estonian Defence and Aerospace Industry Association (EDAIA) was established, connecting enterprises to develop different defence-related solutions (EDAIA, 2024). The strengths of the Estonian defence industry are cyber defence solutions, autonomous systems, sensors, communication and surveillance technologies, electronics, individual equipment, vehicle maintenance and repair (Kaitseministeerium, n.d.)

The Estonian defence innovation policy is based on two principal documents of the Ministry of Defence (MoD) – Research and Innovation Policy (Kaitseministeerium, 2022) and Defence Industrial Policy (Kaitseministeerium, 2021). The main aim of the Research and Innovation is to support innovative solutions such as support command and control, with the prototypes integrated in early phases into the units and supported by tests and analysis of the effectiveness of the use of new technologies. Strong emphasis on cooperation with civilian academic institutions and international cooperation, including cooperation in EU and NATO research and development (R&D) programs. The MoD has already, since 2013, also supported research projects in the defence innovation field through a yearly competition for grants, together with some operational support (Kaitseministeerium, 2022). Defence Industrial Policy sees the defence industry as part of Estonia's defence capability, with a focus on dual-use capabilities and primarily on enhancing the export potential.

Concerning the investments, Russia's full-scale aggression against Ukraine brought along essential changes regarding the funding defence budget; in 2022, decisions on additional funding of more than 1,250 billion euros were made (ECDT, 2023) and eventually, in the National Defence Concept 2023 the whole of the government agreement was reached to raise the defence budget to 3%. For over a decade, Estonia has already shown that it has taken defence needs seriously, which is well reflected in the dedication to contribute 2% of GDP to the defence budget from 2015 onwards (NATO, 2023). The amount dedicated to the innovation in the Estonian defence budget is stable, although not considerable, reaching 1% of the defence budget.

However, when it comes to the current practice of adopting innovative solutions into the Estonian Defence Forces, it has been argued that the uptake is relatively small, mainly because the Estonian Defence Forces is a reserve force based on conscripts, the technological advances capabilities could become too complex for the reservists. In addition, 'there is the absence of long-term strategic foresight, as well as a relatively poor ability to identify deep problems for R&D-based solutions, or sometimes even to articulate effective military requirements' (Jermalavicius, 2021). Therefore, technological innovations are initiated by the Ministry of Defence or industry and, as such, focus rather on technical innovation than on satisfying the operational requirements (ibid).

Estonia's membership in NATO and the European Union and its digital solid base provide opportunities for cooperation and knowledge-sharing with other member states. Estonia has performed, especially considering the size of the country and its ability to invest in innovation, quite well, participating well in EDF projects (MoD, 2023) and is one of the founding members of NATO defence initiatives. It has established a good base for supporting defence innovation in its relevant strategies and policies and, to a certain level, also in practice. By further engaging in multinational defence initiatives, thus accessing a wide range of expertise, technologies, and resources and fostering the defence innovation implementation by Defence Forces, it could create a niche capability contributing significantly to allied security and defence developments. Such a niche would well correspond to the forecasts for future security developments and warfighting both by NATO and the EU, reflected in the NATO Warfighting Capstone Concept and EU's Strategic Compass, and would also encompass the lessons from the war in Ukraine.

Recommendations

The future outlook shows growing (great power) competition and challenges that will also certainly impact Estonia, situated next to aggressive Russia. When looking at the future of defence forces and warfighting, the growing impact of innovation and emerging technologies is highlighted both in NATO and EU documents. The ongoing war in Ukraine also shows the positive impact that new technologies and innovative thinking can have.

Estonia is well-known for being a digital country that highly emphasises cyber, thus forming a good base for technological innovation. Estonia's strategic documents highlight innovation and innovative thinking as essential goals. Estonia has created in its policies and strategies a good base for raising innovation higher into its agenda. However, implementing innovative solutions in the defence field has seen some obstacles, mainly the reserve-based defence forces system. Although acknowledging the need to fill the capability gaps with conventional means and stocks with ammunition, Estonia has the potential to create a niche of innovation that could have added value to Estonia and its allies, especially with the new instruments created to support innovation both in NATO and the EU.

Therefore, following are the ideas to consider:

1. **Create a testbed for innovation:** Estonia could create conditions to serve as a testbed for innovative solutions that would benefit both NATO allies and EU member states. As one solution, specially dedicated innovation-tested units could be established based on broad membership in the Defence League, providing people with different backgrounds.
2. **Invest in technologically (SMET) educated people:** As a highly digitalised country, Estonia has the potential to increase the technological know-how of people through purposeful programs in the secondary schools and defence educational institutions, such as the Estonian Defence Academy and Defence League School, to support the innovation-leaning leaders and member of the Defence Forces.
3. **Encourage further private-public cooperation:** Estonia already has established a Defence League Cyber Unit; similarly, a technology-innovation support group could be established that would serve as civil-military cooperation accelerator.
4. **Adopt innovative technologies:** By integrating new technologies into defence operations, Estonia could optimise decision-making processes, enhance situational awareness, and improve overall defence effectiveness. Especially by sensor systems for enhancing surveillance capabilities and autonomous systems, including unmanned aerial vehicles (UAVs) and unmanned ground vehicles (UGVs) for operational efficiency. At the same time, it could provide the Estonian defence industry with references and thus support the export of innovative technologies.

5. **Increase the investment into R&D:** investing more into R&D would enable to support private companies in developing defence-related solutions and thus enhance the opportunities for capability developments.

Conclusion

Estonia is a small country situated geopolitically next to neighbouring aggressive Russia. According to the literature, the option for a small country to build itself an effective strategy is to choose between shelter-seeking, which could be interpreted as aligning with a strong ally or the alliance, or hiding, also understood as neutrality. The main principles directing Estonian strategy are “Estonia will fight back” and “never alone again”, thus clearly reflecting that it has chosen the option of shelter-seeking in the format of belonging to NATO and the EU.

According to the overview of the successful strategies of the small states, a benefit of the niche capability emerges. Therefore, it would be wise for Estonia to develop a defence strategy that enhances its military capabilities and provides a specific added value to its allies. In this regard, Estonian strategic documents highlight the importance of a solid international position and cyber and innovation. As several successful efforts have been made in the field of international position and cyber, Estonia could next focus more on defence innovation.

The base to establish a niche capability of defence innovation has been well established in the national strategy documents and adopted policies; there are also several companies that focus on innovation in the defence field. Moreover, innovation has a vital role in the future forecasts of NATO and the EU documents that predict the strategic environment and future warfighting. However, it has been referred that the reserve-based defence forces do not fully support the implementation of innovative solutions. At the same time, Estonia has an excellent example of creating a cyber unit in the Defence League, composed of voluntary members, and this also serves as a way forward also for innovation.

NATO and EU initiatives can play a significant role in helping Estonia develop and improve innovation and allied security. Through participation in international frameworks and initiatives, NATO and the EU provide a framework for small states to bolster their security, innovate, and effectively respond to modern threats. Estonia has shown its ability to perform well in NATO and the EU initiatives, and there is also potential for further engagement.

In sum, by creating a niche capability of defence innovation, Estonia could create a successful defence strategy, increase its defence capabilities, and simultaneously offer clear additions to the allies.

Recommendations for defence innovation:

1. Create a testbed for innovation
2. Invest in technologically educated people
3. Encourage further private-public cooperation
4. Adopt innovative technologies
5. Increase the investment into R&D

Bibliography

Allied Command of Transformation (ACT). 2023. NATO. *Strategic Foresight Analysis 2023*. [Online] 2023. [Cited: 22 April 2024.] [SFA2023_Final.pdf \(nato.int\)](#).

Allied Command of Transformation (ACT). 2021. NATO. NATO Warfighting Capstone Concept. [Online] May 2021. [Cited: 22 April 2024] <https://www.act.nato.int/wp-content/uploads/2023/06/NWCC-Glossy-18-MAY.pdf>.

AP News. 2024. World News: Russia puts the leader of NATO member Estonia on a wanted list over the removal of Soviet-era monuments. *AP News*. [Online] 13 February 2024. [Cited: 22 April 2024.] <https://apnews.com/article/russia-estonia-kallas-wanted-list-4ca301df09eace6643be66a9a4a93fe8>.

Atlantic Council. 2019. Purpose of a national security strategy. *Atlantic Council*. [Online] 28 February 2019. [Cited: 22 April 2024] <https://www.atlanticcouncil.org/content-series/strategy-consortium/purpose-of-a-national-security-strategy/>.

Bhatti, Ayesha. 2023. Why the EU should look to Estonia to achieve its vision for a Digital Europe. *Venture for Data Innovation*. [Online] 17 April 2024. [Cited 22 April 2024.] <https://datainnovation.org/2024/04/why-the-eu-should-look-to-estonia-to-achieve-its-vision-for-a-digital-europe/>.

Brands, Hal. 2023. The Indispensable Art: Three generations of Makers of Modern Strategy. [ed]. Hal Brands. *The New Makers of Moderns Strategy*. Princeton and Oxford : Princeton University Press, 2023.

Carr, Andrew. 2024. Strategy as Problem-Solving. *The US Army War College Quarterly: Parameters*. Spring 2024, 1.

Cheung, Tai Ming. 2021. A conceptual framework of defence innovation. *Journal of Strategic Studies*. 2021, Vol 44, 6.

Council of the European Union (Council of). 2022. A Strategic Compass for Security and Defence - For a European Union that protects its citizens, values and interests and contributes to international peace and security. *EUEA*. [Online] 21 March 2022. [Cited: 22 April 2024.] <https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/en/pdf>.

Defence Innovation Accelerator for the North Atlantic (DIANA). About DIANA. NATO. [Online] [Cited: 22 April 2024.] <https://diana.nato.int/>.

Dyčka, Lukáš, Taivo Rõkk And Zdzisław Śliwa. 2020. Defence strategies of the smaller NATO states – a comparative study. *Czech Military Review (Vojenské rozhledy)*. 2020, 29 (4).

E-Estonia. 2024. Facts and Figures. [Online] n.d. [Cited: 22 April 2024] <https://e-estonia.com/facts-and-figures/>.

Estonian Centre for Defence Investments (ECDT). 2023. Defence Investments 2023–2027. [Online] 2023. [Cited: 22 April 2024.] https://www.kaitseinvesteeringud.ee/wp-content/uploads/2023/02/defence-investments_2023-2027veeb.pdf.

Estonian Defence and Aerospace Industry Association (EDAIA). 2024. Cluster and Members. [Online] n.d. [Cited: 22 April 2024.] <https://defence.ee/cluster-and-members/>.

Estonian Foreign Intelligence Service (EFIS). 2024. Estonia in International Security Environment 2024. *Report*. Estonian Foreign Intelligence Service.

Estonian Ministry of Defence (MoD). 2022. News: Estonia chosen as one of the initiators of the NATO DIANA future technologies programme. [Online] 5 April 2022. [Cited: 22 April 2024.] <https://kaitseministeerium.ee/en/news/estonia-chosen-one-initiators-diana-future-technologies-programme>.

Estonian Ministry of Defence (MoD). 2023a. Home: Setting Transatlantic Defence up for Success: A military Strategy for Ukraine's Victory and Russia's Defeat. [Online] 27 December 2023. [Cited: 22 April 2024.] <https://kaitseministeerium.ee/en/setting-transatlantic-defence-success-military-strategy-ukraines-victory-and-russias-defeat>.

Estonian Ministry of Defence (MoD). 2023b. News: Estonia achieves unprecedented success with European Defence Fund projects. [Online] 23 June 2023. [Cited: 22 April 2024.] <https://www.kaitseministeerium.ee/en/news/estonia-achieves-unprecedented-success-european-defence-fund-projects>.

European Commission. 2023. European Innovation Scoreboard 2023. Country profile Estonia. [Online] June 2023. [Cited: 22 April 2024.] https://ec.europa.eu/assets/rtd/eis/2023/ec_rtd_eis-country-profile-ee.pdf.

European Commission. 2024. A new European Defence Industrial Strategy: Achieving EU readiness through a responsive and resilient European Defence Industry. *Joint Communication To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions*. Brussels, 5.3.2024, JOIN(2024) 10 final.

European Defence Agency (EDA). 2022. News and Events: Hub for EU Defence Innovation Established within EDA. [Online] 17 May 2022. [Cited: 22 April 2024.] <https://eda.europa.eu/news-and-events/press-office/latest-press-releases/2022/05/17/hub-for-eu-defence-innovation-established-within-eda>.

European Union External Action (EUEA). 2024. Annual Progress Report on the Implementation of the Strategic Compass for Security and Defence. [Online] March 2024. [Cited: 22 April 2024.] https://www.eeas.europa.eu/sites/default/files/documents/2024/StrategicCompass_2ndYear_Report_0.pdf.

Franke, Ulrike and Söderström, Jenny. 2023. Star tech enterprise: Emerging technologies in Russia's war on Ukraine. *Policy Brief*. European Council on Foreign Relations. [Online] 5 September 2023. [Cited: 22 April 2024.] <https://ecfr.eu/publication/star-tech-enterprise-emerging-technologies-in-russias-war-on-ukraine/>.

Global Innovation Index. 2023. Innovation in the face of uncertainty. *World Intellectual Property Organisation*. [Online] n.d. [Cited: 22 April 2024.] <https://www.wipo.int/edocs/pubdocs/en/wipo-pub-2000-2023-en-main-report-global-innovation-index-2023-16th-edition.pdf>.

Horowitz Michael C. and Pindyck Shira. 2023. What is a military innovation and why it matters. *Journal of Strategic Studies*. 2023, Vol 46,1.

Jermalavičius, Tomas, Hurt Martin. 2021. Defence Innovation: New Models And Procurement Implications. The Estonian Case. *Policy Paper*. ARES Group. [Online] September 2021. [Cited: 22 April 2024.] <https://www.iris-france.org/wp-content/uploads/2021/09/71-Policy-Paper-Def-Innov-Estonian-Case-Sept-2021.pdf>.

Jones Seth G., McCabe Riley, Palmer Alexander. 2023. Ukrainian Innovation in a War of Attrition. *Brief*. Centre for Strategic and International Studies. CS/IC. [Online] 27 February 2023. [Cited: 24 April 2024.] <https://www.csis.org/analysis/ukrainian-innovation-war-attrition>.

Kaitseministeerium. N.d. Defence Research and Development. Riigikaitseareng.ee. [Online] n.d. [Cited: 26 April 2024.] <https://riigikaitseareng.ee/en/defence-research-and-development/>.

Kaitseministeerium. 2021. Eesmärgid, tegevused: Kaitsetööstuspoliitika (Goals, activities: Defence Industry Policy) [Online] 25 May 2022. [Cited: 24 April 2024.] <https://kaitseministeerium.ee/et/eesmargid-tegevused/kaitsetoostuspoliitika>.

Kaitseministeerium. 2022. Eesmärgid, tegevused: Teadus- ja innovatsioonipoliitika (Goals, activities: Research- and Innovation policy) [Online] 25 May 2022. [Cited: 24 April 2024.] <https://kaitseministeerium.ee/et/eesmargid-tegevused/teadus-ja-innovatsioonipoliitika>.

Kaitseministeerium. 2022. Eesmärgid, tegevused: Teadus- ja arendustegevus (Goals, activities: Research and development activities) [Online] 25 May 2022. [Cited: 24 April 2024.] <https://kaitseministeerium.ee/et/eesmargid-tegevused/teadus-ja-arendustegevus/kaitsetoostuse-valdkonna-tegevustoetuste-konkurss>.

Kiel Institute for the World Economy (Kiel Institute). 2024. Ukraine Support Tracker. [Online] 2024. [Cited: 22 April 2024.] <https://www.ifw-kiel.de/topics/war-against-ukraine/ukraine-support-tracker/>.

Meiser, Jeffrey W. 2016. Ends+Ways+Means=(Bad) Strategy. *The US Army War College Quarterly: Parameters*. Winter, 2016, Vol 46, 4.

Muravska, Julia. 2023. Drones and defence innovation in Ukraine: consolidating wartime ingenuity. King's College London. [Online] 29 November 2022. [Cited: 24 April 2024.] <https://www.kcl.ac.uk/drones-and-defence-innovation-in-ukraine-consolidating-wartime-ingenuity>.

NATO Innovation Fund (NIF). About. [Online] n.d. [Cited: 22 April 2024.] <https://www.nif.fund/>.

NATO. 2022. NATO 2022 Strategic Concept. [Online] 3 March 2023. [Cited: 23 April 2024.] https://www.nato.int/cps/en/natohq/topics_210907.htm.

NATO. 2023. Defence Expenditures of NATO Countries (2014-2023). [Online] 7 July 2023. [Cited: 22 April 2024.] https://www.nato.int/cps/en/natohq/news_216897.htm.

Pettyjohn, Stacie. 2023. Evolution Not Revolution. Drone Warfare in Russia's 2022 Invasion of Ukraine. Center for a New American Security. [Online] 8 February 2024. [Cited: 24 April 2024.] <https://www.cnas.org/publications/reports/evolution-not-revolution>.

Praks, Henrik. 2019. Estonia's approach to deterrence. [ed]. Nora Varanga and Toms Rostoks. *Deterring Russia in Europe. Contemporary Security Studies*. London and New York : Routledge, 2019.

RAND Corporation. 2021. Russian Grand Strategy: Rhetoric and Reality. [Online] 16 August 2021 [Cited: 22 April 2024.] www.rand.org/t/RR4238.

Riigikantselei. 2023. National Risk Analysis 2023. [Online] n.d. [Cited: 22 April 2024.] <https://www.riigikantselei.ee/en/risks-past-experiences-and-future-considerations>.

RUSI. 2024. NATO Societies Must be Ready for War. [Online] 26 January 2024. [Cited: 22 April 2024.] <https://rusi.org/explore-our-research/publications/commentary/nato-societies-must-be-ready-war>.

Silove, Nina. 2018. Beyond the Buzzword: The Three Meanings of “Grand Strategy”. *Security Studies*. 2018, Vol 27, 1.

Strachan, Hew. 2006. The lost meaning of strategy. *Survival*. 2006, Vol 47, 3.

Strategy “Estonia 2035”. 2021. [Online] 12 May 2021. [Cited: 22 April 2024.] https://valitsus.ee/en/node/31?view_instance=0¤t_page=1.

Strebel, Paul. 2017. Strategy is dead? Long live strategic thinking! [Online] February 2017. [Cited: 22 April 2024.] <https://www.imd.org/research-knowledge/strategy/articles/strategy-is-dead/>.

The Guardian. 2024. News: Trump says he would encourage Russia to attack Nato allies who pay too little. [Online] 11 February 2024. [Cited: 22 April 2024.] <https://www.theguardian.com/us-news/2024/feb/11/donald-trump-says-he-would-encourage-russia-to-attack-nato-countries-who-dont-pay-bills>.

The New Statesman. 2024. Europe’s Iron Lady: Estonian prime minister Kaja Kallas [Online] May 2022. [Cited: 22 April 2024.] <https://www.newstatesman.com/international-content/2024/02/estonian-prime-minister-kaja-kallas-russia-profile>.

Thorhallsson, Baldur. 2018. Studying small states: A review. *Small States & Territories*. 2018, Vol. 1, No. 1.

TIME. 2022. 2022 TIME100 NEXT: Kaja Kallas. [Online] 28 September 2022. [Cited: 22 April 2024.] <https://time.com/collection/time100-next-2022/6213907/kaja-kallas/>.

Väyrynen, Raimo. 1997. Small States: Persisting Despite Doubts. [ed.] Efraim Inbar and Gabriel Sheffer. *The National Security of Small States in a Changing World*. Frank Cass: London. Portland, OR.

Wivel, Anders. 2021. The Grand Strategies of Small States. [ed] Thierry Balzacq and Ronald R. Krebs. *The Oxford Handbook of Grand Strategy*. Oxford : Oxford University Press, 2021.

VILMANTAS VALANTINAS. Relations between Russia and China in the face of Russia-Ukraine war”

Introduction

After the successful first phases of the Ukrainian army counterattack, which made it possible to reclaim territories in the North-Eastern and South-Eastern parts of Ukraine in the second half of 2022, the counter-offensive has stalled since the beginning of 2023, and the front line has settled in about the same place. Several factors are distinguished that allowed Russia to stabilize the situation on the front and reorient the country's economy for a long war of attrition. The support of other nations is one of the main ones. Undoubtedly, one of the prominent supporters of Russia in the war with Ukraine is China. “China does not share our values; it challenges our interests, and Beijing is increasingly aligned with Moscow” (Stoltenberg, 2024), states NATO General Secretary Jens Stoltenberg in his annual report 2023. The evaluation is given after two years of large-scale Russia-Ukraine (RUS-UKR) war.

Beijing is supporting Russia's military-industrial infrastructure, including by supplying dual-use materials and weapon components, to give economic and security support to Russia's war in Ukraine. Since the beginning of the conflict in Ukraine, trade between China and Russia has increased, and since 2022, exports of commodities from China that may be used in the military have more than tripled.

Due to Moscow's close economic relations with Beijing, Russia has access to a significant market for its commodities and energy, is better protected from further sanctions, and has a more powerful ally in the fight against the United States (US). China is Russia's most significant commercial partner; in 2023, bilateral trade is expected to reach over \$220 billion, nearly 15% higher than the record sum in 2022 (Intelligence, 2024).

From the very beginning of the UKR-RUS war, Chinese officials communicated neutrality, respect for Ukraine's sovereignty, and the necessity to halt the war through

fast-paced negotiations. Nevertheless, the Chinese trade of Russian data has proved the opposite. Although China pretends to be neutral in communicating its position towards the UKR-RUS war, Russia's wartime economic indicators, Chinese materials, equipment, and components of munition used on the battlefield, incontrovertible help to overcome EU and US sanctions, witnessed Chinese solid support to the aggressor. Therefore, this paper will argue how Beijing's official position contradicts what they are doing in the economic and trade field, which mirrors the Chinese stance towards the Russia-Ukraine war and China's rationale behind this.

Divided into three parts, this paper presents the instances illustrating Russia's and China's strategic approaches in the economic, diplomacy, and military fields, excluding their similarities and differences and distinguishing areas where these two powers may find common interests. Subsequently, the second part portrays the Chinese officials' stance toward the Russian invasion of Ukraine and how it evolved during the war, and it excludes areas where these two powers may find common interests. Section three lists Beijing's footprint in assisting Russia to keep the economy to the point where the military industry can continue the war in Ukraine, as well as channels of supply of technology components, materials, and equipment necessary to continue the invasion. This argumentative essay is supported by the analysis of Russia's and China's strategies by authoritative agencies, geopolitical reports on China-Russia relations in the face of the RUS-UKR war in particular, and reliable articles in mass media.

What are the similarities and differences between Russia's and China's strategies?

It is crucial to determine China's and Russia's similarities and differences in their national strategies to understand China's position and actions influencing the course of the Ukraine-Russia war. This chapter examines both countries' foreign policy, economic, and military strategies. It will conclude with similarities, which will lead to the assumption of why it is favorable to cooperate for both Russia and China in the face of the current war.

Russia's strategy

Russian leadership tends to believe that the US-led Western-centric unipolar system is transitioning to a system where power will be allocated more equally between a

broader range of states. Greater global stability and prosperity will result from this transition, which is desirable by Moscow. It will allow Russia to become a major power and a regional leader. Nevertheless, the transition period is expected to increase geopolitical instability and the likelihood of wars. This view holds that the West will act in a destabilizing manner in particular, as it resists the inevitable relative decline. Thus, as immediate threats from the neighborhood emerge, Russia will require a decent military to defend its national interests from multiple threats. Moscow anticipates a return to stability in collaboration with other great powers that respect each other's interests. In addition, Russia will seek to be one of several great power centers, playing a major role in Eurasia with the influence in prominent international organizations (Charap, et al., 2021).

Moreover, the above provisions are reflected in the vision of the former Russian Prime Minister Primakov, known as his doctrine, which has been unwritten per se. It argues that the US cannot dominate a unipolar world and suggests the following principles for Russian foreign policy: 1. The US exercised unipolarity must be changed by multipolarity where major powers, with Russia included, are orchestrating the world order. 2. Russia has a primacy and dominance in the post-Soviet area. 3. Russia opposes any NATO enlargement (Rumer, 2019).

According to Russia's strategy, if new centers of power continue to emerge over the next ten years, and as a result, once-dominant nations like the US strive to maintain their position, there will be an increase in instability in the international order. Therefore, Russia foresees an increase in threats, competition, and instability because it will appear as an effect of Moscow's actions to seek an independent foreign policy to safeguard its regional and global interests. To achieve overarching goals, RAND, in their report, names six elements of Kremlin strategy: 1. There is a growing integration of external and internal risks. 2. Russia intends to take a benign leadership stance in its immediate neighborhood. 3. Russia needs to get ready for border skirmishes and non-contact warfare. 4. Regional projection of power takes precedence over global military expeditionary capacity. 5. The goal is not to undermine the West but to selectively collaborate while containing Western aspirations. 6. Russia plans to shift its focus to "new centers of power" rather than the West (Charap, et al., 2021).

Russia has been gradually implementing these goals since the 2008 annexation of South Ossetia and Abkhazia in Georgia. It has continued its politics through military power in Ukraine since 2014 and Syria in 2015. The most explicit expression of Russian political goals is the large-scale invasion of Ukraine since February 2022, where an aggressor is using all means, including brutal and unconventional, it sees necessary.

Definitely, in achieving multipolarity and its strategic objectives, Russia strives to cooperate with countries that might obey similar interests to withstand Western order as well as to support military conflicts. Russia's strategy outlines intentions to pursue engagement with other Asia-Pacific countries and extensive cooperation with China. Therefore, Russia's economic strategy has had a significant shift from Europe to Beijing since 2014. By the end of 2021, China's and Russia's trade share had increased from around 10% in 2013 to 18% (Graham, 2023).

Additionally, regarding the concept of power, the cooperation between Russia and China in the energy field is of tremendous importance. Experts summed up areas that force countries to cooperate as follows: 1. To maintain their national security, power, and interests, China and Russia are aggressively vying for access to and control over natural resources. 2. Russia's reliance on oil exports makes it more vulnerable. 3. As nations and their national energy firms compete more for natural resources, onshore and offshore joint projects have resulted from this competition (Priorities of Russian energy policy in Russian-Chinese relations, 2020). Moreover, the need to have decent energy resources trade has become even more critical for the Kremlin since the West applied energy trade sanctions after Russia's full-scale invasion of Ukraine.

China's strategy

After the Mao era, China's strategy evolved and realized a strategy focused on achieving great power status. To fulfill that, China has had to apply a "comprehensive national power" approach that focuses on diplomatic, economic, military, and other spheres. Major power status entails command over actions inside China's boundaries, on its territory, and outside its borders, as well as a degree of worldwide influence and strength that upholds and defends the fundamental objectives of national security, development, and sovereignty. Beijing has outlined various objectives related to economic growth, leadership in international security, diplomatic and economic

initiatives, and sovereignty over the territory it claims. Beijing is attempting to strengthen its geostrategic standing diplomatically with the US, other superpowers such as Japan and India, China's neighbors, and emerging nations. China's military goals primarily focus on maintaining its territorial integrity and sovereignty. These objectives often force China into tensions and even direct confrontation with neighboring nations, the US itself, and its partners (Scobell, et al., 2020).

The main instrument of Xi's administration's foreign policy is the Belt and Road Initiative (BRI), which involves and frames most of Beijing's foreign and economic policies and their activities (National, 2015). The initiative entails creating an enormous railways, roads, pipelines, canals, and sea links connecting China to the global community. The objectives are numerous and include increasing China's global influence, projecting the image of growth as constructive and non-dangerous to other nations, engaging in nonconfrontational competition with the US and other superpowers, and, finally, promoting China's economic development (Rolland, 2017). All this strategy is projected to safeguard a modern economy by providing legitimacy for the country's governing party and creating a "moderately prosperous society" for its 1.4 billion residents.

To pursue economic and diplomatic goals, China also organizes its military strategy. The focus of Chinese military objectives is focused on the defense of its national territory and sovereignty. The main component of China's national defense policy, according to the 2000 defense white paper, is "bolstering national defense, resisting invasion, preventing armed overthrow [of the government] as well as defending the sovereignty, territorial unity and security of the nation" (State Council Information Office of the People's Republic of China, 2000). These identical goals have been listed repeatedly in the later defense white papers, with little change. Nevertheless, Beijing has been viewing the US as its primary military challenge at home as well as overseas. Therefore, China's military will undoubtedly conduct operations outside the country, carrying on a long-standing practice of putting relatively small force packages in remote areas. The objective need for the Army's entire domain of combat operations stems from the growth of national interests globally and the whole domain of safeguarding national security. Overseas operations are mostly related to the protection of Chinese interests linked to BRI and other Beijing leadership and population interests globally. However, the authors of the RAND report claim that Xi's priorities are regional rather

than global. China seeks to establish an area where it would exercise influence and deny other great powers' armed forces, primarily the US, access without exposing themselves to significant risk. The occupation or invasion of other areas in the Indo-Pacific is not considered to be Beijing's interest (except the waters in East China and South China seas and Taiwan), but rather the establishment of a China-centric regional order expressed with hard power and soft power is Beijing overarching goal (Scobell, et al., 2020).

In conclusion, the analysis of the strategies of Russia and China shows that the partnership between these two countries is beneficial to each other for different reasons. Russia's strategy aims to partner with countries that have professed non-Western values from the late Yalcins and especially from the early stages of Putin's leadership. China is a very suitable partner for this. Moscow especially encouraged this partnership from an economic, military, and diplomatic point of view in the last decade, when the West imposed sanctions on Russia after the 2014 Crimea and eastern Ukraine annexation. As China has completely different reasons. Despite both Beijing and Moscow identifying the US as an opposing global great power, China's strategy does not foresee Russia as a vital partner in the long run. Experts argue that China has been just using the opportunity to "distract and deplete the US in a secondary theater while it continues to build strength" for a Taiwan invasion (Kine, et al., 2024). It is supported by Marcin Zaborowski, who claims that China, as a majority of great powers, never makes alliances; they use other countries for their own need and interests (Zaborowski, 2024).

What is China's official position towards the RUS-UKR war?

China's stance on the Russian invasion of Ukraine has been contradictory. On the one hand, it has placed the blame on NATO expansion, which Russia claims was the driver for the war's beginning. However, Beijing has emphasized support for Ukraine's territorial integrity. China has abstained from voting on the war in Ukraine at the UN and has not denounced Russia's invasion of Ukraine. The reasons for such official inconsistency might be influenced by many factors, including Beijing's changing assessments of Taiwan's potential implications from the RUS-UKR war, the need to oppose the US, the desire to back Russia while limiting the costs to Chinese interests, the requirement for stability in politics in China, and specific elements of its domestic

system of politics that have an impact on the formulation of foreign policy (Greitens, 2022). This chapter will highlight the main tendencies of Chinese officials' communication on the sanctions the EU and the US applied to Russia, Beijing-Moskow economic relations, and support to Russia by military means.

With the flow of the war, it is possible to recognize the change in the rhetoric of Chinese officials. Just at the beginning of the war in 2022, Mr. Qin Gang, China's ambassador to the US, declared that China's stance is neutral and objective: the goals and tenets of the United Nations Charter must be adhered to in full; respect must be shown for the territorial integrity and sovereignty of all countries, including Ukraine; justifiable security concerns of all nations must be given careful consideration; and all initiatives that promote a peaceful resolution of the conflict must be encouraged (Gang, 2022). After half a year, in September 2022, Mr. Li Zhanshu's stance, who is the highest advisor to Xi Jinping, was not so impartial. He blamed NATO's enlargement towards Russian borders; thus, Moskow has taken an "impossible situation" on the Ukrainian issue (Ramzy, 2022). Finally, at the beginning of 2024, Chinese defense minister Dong Jun, over a meeting with defense minister Sergei Shoigu, already explicitly expressed support for Russia in the Ukraine conflict, despite pressure from Western nations and the possibility of Beijing and the EU's defense cooperation being disrupted (Щербакова, 2024).

Beijing has been reproducing the Russian narrative domestically while muted internationally. For China's 1.4 billion citizens, a reality is presented where the Russian President is a victim defending a humiliated Russia; the invasion is reduced to a "special military operation," and the US may be sponsoring a biological weapons program in Ukraine, as reported by the country's national broadcaster CCTV. Primary state-run news sources, who control most of China's heavily restricted media landscape, have mostly reiterated Russian state media reports from Russian officials to present its narrative (McCarthy, 2022).

From the beginning of the Russian invasion of Ukraine, Chinese officials unsupported the Western sanctions against Moskow. They have condemned those as being unilateral, ineffective, and having illegal backgrounds. The head of the China Banking and Insurance Regulatory Commission did not see the possibility of significant harm for China caused by sanctions on Russia and expressed the intention to continue

having regular trading and commercial relations with pertinent parties (Yao, Kevin , 2022). However, some Chinese financial institutions have restricted Russia's access to their financing systems to avoid direct and secondary Western sanctions (Lo, 2024). Beijing has chosen a minimal communication posture on plausible Chinese military equipment, munition, and other means of export to Russia. Worldwide media reports numerous times suspected China's support to the Kremlin by military means. For instance, Russia's Foreign Intelligence Service (SVR) leaked information about China's intent to pass off military hardware as civilian supplies and authorized the "provision of lethal aid" to Russia in its conflict with Ukraine earlier in early 2023 (DeYoung, et al., 2023). Also, Secretary of the US Antony Blinken, relying on the US intelligence services, accused Beijing's administration of providing arms and ammunition to Russia (Berry, 2023). China's reaction to such claims - "have no factual basis." What is declared by the Chinese Ministry of Commerce is that there is standard practice around the globe to impose export restrictions on high-performance unmanned aerial vehicles that possess specific military characteristics; these measures are not directed against any particular nation. The ministry declared export restrictions on a number of drone-related products, such as anti-drone systems, communication devices, and lasers. Certain consumer drones will also be subject to the restrictions, which went into effect on the 1st of September, 2023. Additionally, no civilian drone may be transferred for use for military purposes (Nan, Zhong, 2023).

Given the change in communication of Chinese official figures concerning the RUS-UKR war, it can be concluded that messaging was more reactive and communication was more adaptive to whom and on what occasion communication was made, then an effort would be made to maintain a certain common line of strategic communication. The most cohesive is the position that serves China's own interests and is in line with the principles of 'Real politics'. An example is Xi Jinping's statement where he does not support the war in Ukraine, but China's long-lasting establishment of peace along the Sino-Russian border cannot be compromised. China is sending a very different message to Russia. Russia's official media reports that China's defense minister informed his Russian counterpart: "We have supported you on the Ukrainian issue even though the US and Europe continue to put pressure on the Chinese side." China's minister responded to the same plea by agreeing to collaborate with Russia on "global security and stability" (Chaguan, 2024). The communication of media outlets controlled

by the Chinese authorities, which broadcast narratives beneficial to Russia to local audiences, serves to prove China's apparent support for the Kremlin in this war.

How does China support Russia in the RUS-UKR war?

It differs in the strategy China communicates and what it exercises. For instance, they say that they are keeping a low profile and are not going to expand geopolitically, but on the other hand, starting with the Xi era, China's expenditure on security has grown exponentially, and it has expanded militarily and economically by building bases, investing in infrastructure in Asia, Africa, and Europe (Berzina-Cerenkova, 2024). The difference in communication and behavior has been evident in China's stance towards the RUS-UKR war since the beginning. This chapter will offer an overview of areas in which China has been involved in boosting Russia's military potential and ability to keep initiative on the battlefield, as well as an outlook on how Beijing helps mitigate Western sanctions' effect on the Russian war-centric economy.

China's support to Russia by materials and equipment needed on the battlefield.

China supports Russia massively in the war with Ukraine (Rácz, 2024). Open-source trade data indicates that Russia's capacity to reinforce its fortifications on Ukrainian territory and to maintain them stocked and prepared to stave off the counteroffensive was greatly aided by a spike in imports of Chinese-manufactured commodities with significant military applications. Following the attack on the initial phase of the war in Ukraine, Russia effectively shifted to a defensive stance, dug in on Ukrainian territory, and has been able to maintain its forces there despite ongoing significant losses of military hardware and massive ammunition expenditures. The great majority of items included in this crucial support for Russia's military structure are given freely and are not subject to restrictions or prohibitions by the international sanctions regimes that are in place against Russia. It is evident that the material being offered has a wide range of applications and is crucial to Russia's military campaign (Garlauskas, et al., 2023).

Digging equipment manufactured in China has physically assisted Russia in enforcing its military positions within the occupied area of Ukraine. Massive increases in the import of vehicles, particularly super heavy trucks, have made it possible for Russia's military sector to keep manufacturing the kinds of vehicles necessary to sustain combat strength for a defense in depth. Chinese excavator shipments to Russia more than

tripled in September 2022, corresponding with the Surovikin Line's development. Trench-digging equipment supplies from China to Russia peaked in September 2022 and continued for the rest of the winter (Garlauskas, et al., 2023). Chinese all-terrain vehicles have already been observed on the front lines for one year (Rácz, 2024). Additionally, Russian military logistics can maintain supplies and equipment flowing to the front thanks to Chinese trucks. In the first eight months of this year, Chinese shipments of very heavy vehicles, weighing more than twenty tons, to Russia have increased by 728 percent from 2021 levels (Reuters, 2023).

It is widely discussed about drones' significant role in the RUS-UKR war and the importance of the advantage of warring part in this field. China exports drones to both Russia and Ukraine, but those for Russia are more advanced and newer generations than those arriving in Ukraine (Rácz, 2024). According to a Radio Free Europe/Radio Liberty investigation, Russian military-industrial complex affiliates are purchasing drones made by Chinese company DJI. Cheap drones are supplied to Russian organizations that are a part of its extensive military-industrial complex or to businesses in the nation that instruct military or government personnel in the usage of unmanned aerial vehicles (Standish, 2023). Additionally, in this field, it was revealed that one part of the Iranian-made drone, "Shahed", which has terrified the country's civilian populace, was manufactured in China (Nissenbaum, 2023).

Also, the Ukrainian military has discovered that many of the electronics in Russian weapons that were captured on the battlefield were made in China. A Russian cruise missile is one of these instances of Chinese components used in deadly weapons, as well as Chinese parts used in Russian tanks and "Orlan" aerial drones (Solomon, 2023). Lastly, China has also been supplying important high-tech parts for military use, such as fighter-jet engine parts and avionics, which the US intelligence community has shown in reports available to the public (Intelligence, 2023).

Besides, Chinese businesses have allegedly shipped drones, body armor, and assault guns to Russia covertly, despite Beijing officials having constantly denied that (Kolodii, et al., 2024). Also, Chinese nitrocellulose exports to Russia have grown exponentially since 2022 (Rácz, 2024). Nitrocellulose is a highly flammable compound that is the main ingredient of modern gunpowder, though it is critical for the exploitation of

munition manufacture. Chinese companies provided one-third of the overall supply of this substance in 2023.

China's role in mitigating the negative impact of Western sanctions on Russia.

Sanctions for Russia have a significant influence, but Russia is quite inventive in controlling them or at least minimizing the effect. After Russia invaded Ukraine on the 22nd of February in 2022, the EU and the US introduced various sanctions to influence Russian incomes in the economic field, on the imports of the technologies that might be used in manufacturing weapons or pieces of equipment, sanctioned oligarchs, and other people who support the Russian war machine. Russia's diplomatic efforts to find international partners to bypass the sanctions have given tangible results. China has appeared as one of the most reliable partners because of similarities in viewing international order and opposition to the US.

EU and the US imposed dozens of packages of sanctions on Russia since 2014 and later after 2022. Sanctions are fines imposed on another nation by one to deter it from behaving aggressively or violating international law. These are some of the most challenging actions that a country may do, short of starting a war (News, 2024). Therefore, Moscow shifted the policy to reorient the Russian economy toward Beijing and away from Europe. Their different economies were extensively integrated as a result of the reorientation. China's percentage of all trade with Russia increased from around 10% in 2013 to 18% by the end of 2021 (Graham, 2023).

In June 2022, the EU Council approved a sixth round of sanctions prohibiting the EU from importing or buying natural gas and certain petroleum products from Russia by sea (EU, 2024). Because of that, Russia has increased its energy exports to China to make up for lost market share in the West. By boosting its expenditure on Russian energy from \$57 billion the year before the invasion to \$88 billion the year after, Beijing has given Moscow permission to alter its revenue on the EU market. It goes without saying that the price of crude oil on the global market determines how much money oil products may bring in, and for the Russian economy to be successful, the cost per barrel must be more than \$40–45. Natural gas is another item that China buys from Russia for energy purposes. Since natural gas relies more on currently installed infrastructure, importing more of it quickly is more challenging. By 2023, China is anticipated to receive 22 billion cubic meters of natural gas from Russia; by 2027, this

amount is predicted to reach its maximum capacity of 38 billion cubic meters (Nikoladze, et al., 2023).

Also, China is reducing the negative impact of the sanctions on Russia by providing Moscow with an alternative currency for trade. The Chinese yuan surpassed the US dollar as the most traded currency in Russia at the beginning of 2023. The switch was done in response to US sanctions against a few Russian banks that were still allowed to carry out cross-border dollar transactions. The world's major currencies, such as dollars, euros, and yen, are restricted from being used by Russian financial institutions due to Western sanctions. As a result, the yuan is the only relatively stable and widely traded currency issued by a non-sanctioning authority that allows Russia to conduct international transactions. Consequently, Russia has been able to control the ruble's value through foreign exchange operations with reserves valued in yuan. In addition, Russia raised the amount of yuan allowed in its National Welfare Fund to 60% last year and intends to sell more of the currency to mitigate the budget deficit and compensate for lost energy earnings (Nikoladze, et al., 2023).

Energy resource export to China and usage of yuan for international transactions even resulted in the country's GDP growth of 2,6 percent (Foucart, 2024) this year are several of the most important reasons for Russia allowing to sustain its economy at a decent level to keep the war machine running an attrition fight in Ukraine. However, the lack of supplies from Western businesses to continue high-technology manufacturing is hurting Russia's market. It is crucial, particularly in the armed forces. Therefore, Russia's government endorsed the "parallel imports" approach (Smagin, 2023). In such a way, Beijing's assistance in technology brought a tremendous negative impact on Ukrainian fighting forces. Russia might develop and implement much more advanced military equipment. Therefore, there is an area for the EU and US to overthink how to restrict Chinese technology flow to Russia for use for military purposes. As three Chinese firms have been placed on the sanctions list by the European Union due to their assistance in Russia's conflict against Ukraine (Kine, et al., 2024), it might be considered a proper beginning in jeopardizing Moscow-Beijing cooperation in this field.

In a nutshell, for a moment, China's support for Russia with the exports of materials, technologies, and equipment, mitigating EU and US sanctions effect plays a vital role

in Russia's combat readiness level today and ability to keep countries economy at a sufficient level to fight a long-lasting war with Ukraine. There might be several reasons that motivate China. Despite differences between Moscow's and Beijing's long-term objectives, Russia will exploit China's opportunistic chance to keep Western powers involved in Russia's and Ukraine's war. By supporting the Kremlin's efforts to mitigate sanctions' harm to the country's economy, thus allowing the war industry to be sustained to wage attrition war in Ukraine (Foucart, 2024). Furthermore, Beijing is aware that the loss of Russia might have a negative impact on its own geopolitical standing. China, for this reason, opposes anti-Russian sanctions and backs Russia in waging the war using unrestricted means. This entails considerably boosting trade volumes and providing Russia with dual-use goods, electronic components, and spare parts for use in assaults on Ukrainian military and civilian targets (Service, 2024). Beijing's leadership has been motivated to support Russia because of opportunistic resource gain in the short term, which is critical for China's industry and people's needs. However, there will probably be unfavorable overall economic effects in the medium to long run, particularly for China. The global economy, which is a vital component of China, will suffer from the human and financial consequences of war and foreseen targeted sanctions (Bourgeois-Fortin, et al., 2022). On the other hand, China avoids supporting Russia openly because such an arrangement would make it more difficult to resume commercial connections with Western nations and harm China's reputation among emerging countries as a neutral and fair nation. Furthermore, China adheres to the concept of territorial integrity and does not recognize the seized lands of Ukraine as belonging to Russia (Service, 2024). Also, a significant amount of Chinese foreign-currency reserves is being secured in the US (Chiang, 2022). Therefore, China has been seeking support Russia up until the level of not surpassing the threshold of facing open opposition in the global arena.

Conclusions

Since the beginning of the war in Ukraine, after the EU and the US applied sanctions on the Russian trade and financial system, which challenged Russia's success on the battlefield, Moscow turned for support to international partners with similar values or interests, and China was one of them. Meanwhile, China has taken a controversial official position about the RUS-UKR war. Although China pretends to be neutral in communicating its position towards the war, Russia's wartime economic indicators, Chinese materials, equipment, and components of munition used on the battlefield,

and incontrovertible help to overcome EU and US sanctions witnessed Chinese solid support to the aggressor. Despite China's and Russia's strategic approaches and goals differing significantly, China sees its alliance with Russia as part of a bigger plan to create a worldwide network that functions according to Chinese rules. However, its senior officials and diplomats have been inconsistent in their views on working with Russia in the face of the RUS-UKR war. Beijing messaging was more reactive, and communication was more adaptive to whom and on what occasion communication was made, then an effort would be made to maintain a specific common line of strategic communication. The most cohesive is the position that serves China's own interests and is in line with the principles of 'Real politics'.

China's assistance to Russia in the form of technology, material, and equipment exports, as well as the reduction of the impact of EU and US sanctions, is crucial to Russia's current state of combat preparedness and its capacity to maintain an economy strong enough to conduct a protracted war with Ukraine. Beijing understands that losing Russia may hurt its own position in the geopolitical arena. China, for this reason, opposes anti-Russian sanctions and backs Russia in waging the war using unrestricted means. This entails considerably boosting trade volumes and providing Russia with dual-use goods, electronic components, and spare parts for use in assaults on Ukrainian military and civilian targets. Worth nothing, China's support for Russia has been limited and leveraging on the threshold of facing open opposition in the global arena.

It should be crystal evident to the US, NATO, and their friends and allies worldwide that goods made in and exported from China to Russia are balancing the flow of Western arms and equipment to Ukraine. Even while China does not directly supply Russia with weapons, it does supply materials and equipment that enable Russia to continue its war and annex Ukrainian land. The West should tighten the implementation of export controls throughout Europe, North America, and the Indo-Pacific region and remove leaks from their own sanction regimes. However, given the scale of the Chinese economy, Beijing's hostility against the rules-based international system, and the intricate challenges confronting constitutional democracy, countering Chinese exports to Russia is a challenging issue.

Bibliography

Berry, Lynn. 2023. [Online] February 20, 2023. <https://www.independent.co.uk/news/world/europe/antony-blinken-china-arms-russia-war-b2285558.html>.

Berzina-Cerenkova, Una. 2024. The People's Republic Of China And Its Impact On The International Security Environment. *Lecture for BALTDEFCOL HCSC*. 2024.

Bourgeois-Fortin, Camille, Darren, Choi and Sean, Janke. 2022. *China and Russia's invasion of Ukraine: Initial responses and implications*. s.l. : University of Alberta, 2022.

Chaguan. 2024. The Economist. [Online] 02 08, 2024. <https://www.economist.com/china/2024/02/08/xi-jinpings-chaos-loving-friends>.

Charap, Samuel, et al. 2021. *Russian Grand Strategy*. Santa Monica: RAND Corporation, 2021.

Chiang, Min-Hua Chiang. 2022. The Heritage Foundation. [Online] 3 October 2022. <https://www.heritage.org/global-politics/commentary/why-china-not-all-supporting-russia>.

DeYoung, Karen and Missy, Ryan. 2023. The Washington Post. [Online] April 13, 2023. <https://www.washingtonpost.com/national-security/2023/04/13/russia-china-weapons-leaked-documents-discord/>.

EU. 2024. Council of the European Union. [Online] February 2024. [Cited: February 29, 2024.] [https://www.consilium.europa.eu/en/policies/sanctions/restrictive-measures-against-russia-over-ukraine/sanctions-against-russia-explained/#:~:text=As%20part%20of%20the%20economic,\(due%20to%20import%20restrictions\)..](https://www.consilium.europa.eu/en/policies/sanctions/restrictive-measures-against-russia-over-ukraine/sanctions-against-russia-explained/#:~:text=As%20part%20of%20the%20economic,(due%20to%20import%20restrictions)..)

Foucart, Renaud. 2024. The Conversation. [Online] 2024. <https://theconversation.com/russias-economy-is-now-completely-driven-by-the-war-in-ukraine-it-cannot-afford-to-lose-but-nor-can-it-afford-to-win-221333>.

Gang, Qin. 2022. The Washington Post. [Online] March 15, 2022. <https://www.washingtonpost.com/opinions/2022/03/15/china-ambassador-us-where-we-stand-in-ukraine/>.

Garlauskas, Markus, Joseph, Webster and Emma, C. Verges. 2023. Atlantic Council. [Online] November 15, 2023. <https://www.atlanticcouncil.org/blogs/new-atlanticist/chinas-support-for-russia-has-been-hindering-ukraines-counteroffensive/>.

Graham, Niels. 2023. Atlantic Council. [Online] January 2023. <https://www.atlanticcouncil.org/blogs/econographics/russian-finance-pivots-east/>.

—. 2023. *Russian finance pivots East*. s.l. : Atlantic Council, 2023.

Greitens, Sheena Chestnut. 2022. China's Response to War in Ukraine. *Asian Survey*. 2022, Vol. 62, 5-6.

Intelligence, Office of the Director Of National. 2024. *Annual Threat Assessment Of The U.S. Intelligence Community*. 2024.

Intelligence, Office of The Directorate of National. 2023. *Support Provided by The People's Republic of China to Russia*. s.l. : July, 2023.

Kine, Phelim and Stuart, Lau. 2024. Politico. *Politico*. [Online] 2024. <https://www.politico.eu/newsletter/china-watcher/chinas-russia-support-strategy/>.

Kolodii, Roman, Giangiuseppe, Pili and Jack, Crawford. 2024. RUSI. [Online] March 1, 2024. <https://rusi.org/explore-our-research/publications/commentary/hi-tech-high-risk-russo-chinese-cooperation-emerging-technologies>.

Lo, Kinling. 2024. [Online] February 11, 2024. <https://web.archive.org/web/20240211131858/https://www.scmp.com/news/china/diplomacy/article/3251675/chinese-banks-refrained-dealing-russia-over-sanctions-fears>.

McCarthy, Simone. 2022. CNN News. [Online] March 10, 2022. <https://edition.cnn.com/2022/03/10/china/china-russia-disinformation-campaign-ukraine-intl-dst-hnk/index.html>.

Nan, Zhong. 2023. China Daily. [Online] 08 01, 2023. <https://webcache.googleusercontent.com/search?q=cache:qkhk2YI2eXYJ:https://global.chinadaily.com.cn/a/202308/01/WS64c7e5fea31035260b819839.html&hl=en&gl=us>.

National, Development and Reform Commission of the People's Republic of China. 2015. Vision and Actions on Jointly Building Silk Road Economic Belt and 21st Century Maritime Silk Road. Beijing : s.n., 2015.

News, BBC. 2024. BBC. [Online] February 2024. <https://www.bbc.com/news/world-europe-60125659>.

Nikoladze, Maia, Phillip, Meng and Jessie, Yin. 2023. Atlantic Council. [Online] 2023. <https://www.atlanticcouncil.org/blogs/econographics/how-is-china-mitigating-the-effects-of-sanctions-on-russia/>.

Nissenbaum, Dion. 2023. The Wall Street Journal. [Online] June 12, 2023. <https://www.wsj.com/articles/china-helps-iran-supply-drones-to-russia-quickly-investigators-say-dd492264>.

Priorities of Russian energy policy in Russian-Chinese relations. **Meynkhard, Artur. 2020.** s.l. : International Journal of Energy Economics and Policy, 2020.

Rácz, András. 2024. Conference on Russia. Tartu: s.n., 2024.

Ramzy, Austin. 2022. The New York Times. [Online] September 11, 2022. <https://www.nytimes.com/2022/09/11/world/russia-says-that-a-senior-chinese-official-expressed-support-for-the-invasion-of-ukraine.html>.

Reuters. 2023. [Online] September 23, 2023. <https://www.reuters.com/world/europe/russia-ramps-up-output-some-military-hardware-by-more-than-tenfold-state-company-2023-09-19/>.

Rolland, Nadege. 2017. *China's Eurasian Century? Political and Strategic Implications of the Belt and Road Initiative*. Seattle: National Bureau of Asian Research, 2017.

Rumer, Eugene. 2019. *The Primakov (Not Gerasimov) Doctrine in Action*. s.l. : Carnegie Endowment For International Peace, 2019.

Scobell, Andrew, et al. 2020. *China's Grand Strategy*. Santa Monica: RAND Corporation, 2020.

Service, Estonian Foreign Intelligence. 2024. *International Security And Estonia*. 2024.

Smagin, Nikita. 2023. *Is the Blossoming Relationship Between Russia and the UAE Doomed?* 2023.

Solomon, Jay. 2023. Semafor. [Online] May 30, 2023.
<https://www.semafor.com/article/05/29/2023/after-finding-chinese-chips-in-russian-weapons-ukraine-confronted-beijings-envoy>.

Standish, Reid. 2023. Radio Free Europe/Radio Liberty. [Online] October 5, 2023.
<https://www.rferl.org/a/russia-ukraine-chinese-drones-training-centers/32621432.html>.

State Council Information Office of the People's Republic of China, State. 2000.
State Council Information Office of the People's Republic of China. 2000.

Stoltenberg, Jens. 2024. *The Secretary General's Annual Report 2023*. Brussels: North Atlantic Treaty Organization, 2024.

Yao, Kevin. 2022. Reuters. [Online] 2022.
<https://www.reuters.com/markets/europe/china-banking-regulator-sees-limited-impact-sanctions-russia-2022-03-02/>.

Zaborowski, Marcin. 2024. Conference on Russia. Tartu: s.n., 2024.

Щербакова, Ирина. 2024. Ukrinform. [Online] January 31, 2024.
<https://ura.news/news/1052728379>.

**BEST ESSAY OF THE COMMAND SENIOR ENLISTED LEADER'S COURSE
(CSELC).**



JANE ANDERSEN. Danish strategic challenges in the Baltic Sea after NATO's expansion with Finland and Sweden.

Introduction

Traditional Danish thinking has always been, that Denmark has a big responsibility in the Baltic Sea due to its geographical location. Every passage from the Baltic Sea to the North Sea or the North Atlantic is passing through the Danish straits. The Danish Islands of Bornholm and Ertholmene are placed centrally in the Baltic Sea, and therefore has a strategic importance. If the islands fell in Russian hands, it would extend the reach of the Russian Navy and Airforce. The islands themselves have a geostrategic value as e.g., forward staging point, hence, the Soviet Union in 1946 demanded that no foreign troops were to be stationed on the islands if the sovereignty of the islands were to be given back to Denmark.

Since the beginning of the war in Ukraine, the security situation in the Baltic Sea, has changed significantly. Both Finland and Sweden applied for NATO-membership on 18th May 2022. Finland is now a NATO member, and it is expected, that Sweden will get acceptance soon. Following Finland and Sweden's acceptance into NATO, the Alliance's borders to the east will be significantly shifted. Moreover, the Russian Baltic Fleet, primarily based in and around St. Petersburg, will experience a significant change as it will have to pass the NATO-dominated and controlled waters starting at their doorstep in The Gulf of Finland. On the other hand, Russia still controls the exclave, Kaliningrad, which provides Russia with their only direct access to the Baltic and serves as a forward operating base.

Denmark has several challenges as it is a small state but a large realm and must prioritize the capabilities to protect the Straits, Bornholm, and critical underwater infrastructure as well as protecting Danish sovereignty in the Arctic and the Faroe Islands. As for the Faroe Islands, Denmark, and the Faroe Islands in 2022 agreed to install an Air Surveillance Radar which forms a part of NATO's Integrated Air Defence System. Finland and Sweden also have interests in the Baltic Sea, as they have Oland and Gotland. All three nations have the seabed and critical infrastructure as common interests. It is an extra challenge, that Denmark has contributed with ammunition,

weapons, training etc. to Ukraine during the war which has resulted in a more hostile attitude from Russia.

The question now is whether Denmark's strategic focus should be adjusted as Danish strategic focus, and the capabilities in many years has been looking towards international missions and the navy capabilities are planned according to the former security strategies. The essay will primarily focus on the maritime domain in the Baltic Sea and Danish straits, and only capabilities of Sweden, Finland, and Denmark.

How should Denmark adjust its strategy and capabilities in the face of a new strategic challenge?

Historical background

After World War II, Denmark tried to stay neutral, for the sake of playing a diplomatic role between east and west, even after NATO's establishment and as a founding member. Therefore Denmark began with limitations to the membership. However, this was mostly for domestic reasons. NATO was entered with agreements of no foreign troops or bases or nuclear weapons on Danish soil, and a small defence budget. Despite that, Denmark with its strategic and geopolitical place on the map, has been a vital member and 'later in the post-Cold War period, it proved to be one of the Alliance's most reliable and active members' (NATO, Year unknown).

Since the end of the cold war in 1989 and the Soviet Union collapse in 1991, Denmark like so many others, had many cuts to the defence budget. Denmark discarded their fast attack crafts in 2000, and their submarine capabilities in 2004. However, new frigates entered the navy in the beginning of 2010's, as a replacement for the old and partly obsolete corvettes. The frigates' primary role is area air defence and was a part of the former security strategy where one of the main focuses was international conflicts and smaller capabilities was acquired or retained for coastal operations (Danish Ministry of Defence, MoD, 2004 pp. 8-10). At that time, the development of the welfare state was prioritized, and the parliament did not acknowledge the potential risks from Russia.

The relationship between Russia and Denmark has been of a diplomatic and economic nature, but since the annexation of Crimea, Denmark has been a part of economic sanctions against Russia and the diplomacy has become more strained. Furthermore,

Denmark is one of the most active contributing nations to Ukraine in both economical, humanitarian, and military ways.

Danish partnerships

Denmark is a member of NATO, EU Defence Cooperation and Nordic Defence Cooperation. Up until now on, one of Denmark's closest partners in NATO has been the US. But with the war in Ukraine, other conflicts on the globe and the new members of NATO, these partnerships will probably change as US might leave a bigger part of the responsibility to Europe regarding the Baltic Sea. Denmark will have to increase capability to deal with strategic tasks.

It is important for Denmark to have allied partners as the Danish society is built on these partnerships. Denmark signed the Helsinki agreement in 1975 together with 35 other nations, including the Soviet Union and the US (Helsinki-Komité, Den Danske, Year unknown). This agreement contains the core values which define the Danish mentality and law, including sovereignty of states, human rights, use of power, just to mention a few. Denmark needs partnerships to keep its security and independence. Especially in the current situation where threats to NATO and Europe are more present.

Defence cooperation in Europe consists of different organizations. The main ones are European Defence Cooperation and NATO, while the Nordic countries are further organized in Nordic Defence Cooperation (NORDEFECO). 'The overall purpose of NORDEFECO is to strengthen the participants' national defence, explore common synergies and facilitate efficient common solutions' (NORDEFECO, 2023). The Nordic nations, Finland, and Sweden were not NATO members before Russia attacked Ukraine. Sweden, Finland, and Denmark have several common interests in the Baltic Sea as all three nations have islands with geopolitical interest for both Russia and the nations themselves as well as critical underwater infrastructure. Denmark as a member of the EU had opt-outs regarding Defence Cooperation.

Facing common interests and challenges, it is necessary for partnership members to cooperate. Right now, the Danish Navy has limited capacity for coastal operations and needs capabilities for anti-submarine operations (Kristensen, et al., 2022 p. 87). It is therefore important, that Denmark and its alliance partners cooperates in defining what is needed to survey and defend the Baltic Sea area in all its dimensions.

In May 2022 Sweden and Finland handed in their applications for NATO membership. Finland was quickly admitted as a member, but Sweden is still waiting for the final ratification. Both countries have been discussing whether to join or not for several years, but they have been a part of the Partnership for Peace Programme since 1994 (Pesu, 2023). Furthermore, both countries have participated in NATO missions throughout the years. But with Russia's demonstrated willingness to use military force, every nation must consider the risks. The opinion in both countries was now to join NATO as soon as possible. The same can be seen in Denmark, where on 1st June 2022 an overwhelming majority chose to abolish the EU defence cooperation opt-out in a referendum. Both Finland and Sweden's applications and the result of the EU-defence referendum in Denmark shows, that the mindset amongst the three populations were changed in a very short time. Furthermore, the Danish Parliament decided to increase the defence budget immediately. In the upcoming defence settlement, it is decided to increase to 2 % of GDP within the next 10 years, which also shows that the politicians focus shifted quite fast. According to the Danish constitution, it is important to secure democracy, and that the civil rights inviolability (Folketinget, Year unknown). The value within the democracy is the common foundation of all the Nordic countries and when there is no perceived threat, it is easy to ignore security policy. In many years Danish focus was on the welfare state. The freedom was taken for granted and the society might have been a little more idealistic than realistic. Especially Sweden and Denmark neglected their own security (Lucas, et al., 2023 p. 8). The values of democracy, freedom, civil rights as stated in the Danish Constitutions dated 5th June 1849, is the foundation of all Danish laws, including the Law of Danish Defence. Moreover, many of the same values can be found in the Helsinki agreement. When Denmark (and Sweden and Finland) recognised the threats close to their borders, the big changes in mentality was seen. To fulfil NATO Article 3, which states, that 'Each NATO member country needs to be resilient in order to withstand a major shock such as a natural disaster, failure of critical infrastructure, or a hybrid or armed attack' (NATO, 2023), it is important, that all nations shows preparedness. This sudden awareness resulted in the upcoming increased defence budgets.

After 24. February 2022 – Russia attacks Ukraine.

In late 2021 and early 2022 Russian war rhetoric and staging of military equipment along the Russo-Ukrainian border and in Belarus, could only be interpreted as a precursor to war. As a result of that Denmark deployed a Frigate to the Baltic Sea, in early January 2022 (Danish Ministry of Defence, MoD, 2022). As we all know, Russia attacked Ukraine on the 24th of February 2022.

Several nations across the globe implemented sanctions on Russia, following their attack on Ukraine, a sovereign state. And of course, Denmark was a part of that as well. The balance of power in the world changed, and Denmark being a small state was at great risk, due to its geostrategic position on the map. 17th June 2022 early morning, a Russian corvette violated Danish territorial waters at Ertholmene twice, the same weekend most of the Danish politicians were gathered for the annual political festival to celebrate democracy (Frigaard, 2022).

In September 2022, the Nord Stream natural gas pipeline exploded. Nord Stream runs through the Swedish and Danish exclusive economic zone (EEZ). The pipelines are a part of Europe's critical infrastructure, and the Danish navy immediately dispatched offshore patrol vessels on patrol in the area. It is perceived as an act of sabotage; however, the incidents are still unsolved. There could be several motives, but in my opinion, one could be, to scare the populations and raise energy prices. At the time of writing this essay it happened again one year after Nord Stream; the Balticconnector pipeline between Finland and Estonia is under investigation for 'potential act of sabotage' (Cooban, 2023).

Denmark have made a great deal of contributions to Ukraine. The donations include military support (weapons, ammunition, missiles for air defence etc.), humanitarian and financial support and support for reconstruction (Kriseinformation.dk, 2023). One of the larger donations consists of 19 F-16 fighter jets. This as well as Danish participation in sanctions against Russia means, that the Danish-Russian diplomatic relations have cooled down (Danish Defence Intelligence Service and Police Intelligence Service, 2022). One high level risk is the risk of cyberattack, and the numbers has increased in 2022 and 2023 mainly from pro-Russian hackers (Center for Cyber Security, 2023). In April 2022 15 Russian diplomats were expelled from Denmark due to espionage (Westersø, 2022). In September 2023 the Danish government has ordered Russia to

downsize further 10 diplomats at the Russian embassy in Denmark for the same reason and only 5 diplomats remain (Asmussen, 2023).

Geopolitical and strategic importance of Danish straits

Until now Russia has had direct access to the open sea through the Danish Straits which are international waters. One strait, Oresund, between Sweden and Denmark are shared and under the Copenhagen Convention in 1857, Abolition of the Sound Toll. According to the Territorial Sea Convention from 1958 (United Nations, 1958), which ratifies previous conventions, straits are international waters and innocent passage is legal. Warships was not specific mentioned in the agreement from 1858, but transit passage has always been generally accepted. According to the Sea Convention it is legal to transit, and submarines must be at surface (Christensen, 2000 p. 39). This means, that Russia can legally pass Danish straits if they comply with the Sea Convention. Later, in 1982, UN made a convention, where transit is allowed, sub-surfaced as well, except for Danish and Turkish straits (the Bosphorus Strait and Dardanelles). Passage through the Bosphorus Strait and Dardanelles is regulated in the Montreux Convention of 1936 and gives Turkey the control (Pike, 2021). In this case, Russian warships are allowed to pass in and out of the Black Sea, but only to return to homeport (Ghaedi, 2022) and passage of all non-Black Sea nations has a lot of restrictions. These two conditions give Russia a strategic advantage. The challenge will be if Russia says the warships are going back to base, but instead they participate in the ongoing war. Just after beginning of the war in Ukraine, Turkey was not ready to cut the diplomatic ties to Russia. If the conventions are not being complied with, it is then to consider what the consequences should be and how they are to be handled. NATO has, because of Turkish right to control their straits, more control in the Black Sea than in the Baltic Sea, which means, that Denmark should put a great deal of focus to secure Danish straits as Russia should not have uninterrupted access. Denmark do not have the same laws and conventions to their straits as Turkey, but the strategic challenges could be the same. If the current conflict spreads to the Baltic Sea, the question is if Denmark should be allowed to enforce the conventions of passage from foreign states through Danish straits. And if the conventions are being violated, what would the sanctions be.

With the Finish and Swedish membership of NATO, the first line of defence from a Nordic point of view, has moved further east. With Finland and Sweden's presence to

the east, Denmark can put their effort towards the Danish straits and increase their presence in the Arctic, Greenland, and Faroe Islands. Neither Finland, nor Sweden has coastline to the Norwegian Sea nor the Barents Sea in the Arctic area, which means, that these two nations should focus on the Baltic Sea.

Additional naval capabilities

The Finnish navy currently have 86 ships primarily within the mine warfare domain. Sweden on the other hand, have 50 ships and 5 submarines. The Danish Navy consists of 23 ships (Kristensen, et al., 2022). The Finnish and Swedish navies are composed based on their strategic needs when they were not a member of NATO, whereas Denmark, as a founding member of NATO, has constructed its navy according to the needs of a bigger alliance/NATO's force goals. Denmark needs to be a part of an alliance to defend the nation. However, over the last decades Denmark has not fulfilled the agreements and NATO's Capability Review 2022 shows delays and lack of military capacities (FMN, 2023).

To analyse the threats and needs in the future in the Baltic Sea we must look at the Russian capabilities. The Russian Baltic Sea Fleet consist of approximately 50 ships, including 2 submarines. Most of the fleet has not been modernised since the cold war ended. But they can still play an important role with their anti-access/area-denial (A2/AD) capacity in the area (Nordenman, 2018 p. 2). Because of the size and shape of the Baltic Sea, their A2/AD missiles are a threat to all countries in northern Europe. Positioned in Kaliningrad they were to be a threat to NATO's access to the three Baltic countries and Poland (Williams, 2017). At the same time, long-range anti-ship and land attack missiles could be carried on small vessels as well. As we have already seen, the threats to critical underwater infrastructure as an actual threat and it is therefore necessary to find ways to protect those.

According to those threats it is necessary for NATO and Denmark to consider what is needed to defend and deter. If Denmark chooses to reinstate the submarine capacity, it will take many years until the capacity will be operational. Denmark (and NATO) must therefore rely on partnerships with the capability to operate sub-surface. Denmark has two frigates configured for anti-submarine warfare and three area defence frigates. It is doubtful whether they are capable and resilient to resist for a longer period as they need personnel and training. To monitor the seabed and critical infrastructure, strategic

sensors could be placed in our EEZ. Because of the threats from Russia's long-range ballistic missiles, Denmark needs radars for surveillance and warning. Radars placed on Bornholm and maybe in Finland as well should cover the Baltic Sea as far east as possible to give early warning. The frigates therefore need to be upgraded with capable missile defence systems. With mobile long-range land based coastal missile batteries it would be possible to defend against threats from the sea including threats to the Danish straits. Moreover, those batteries could be a part of deterrence as a kind of fleet in being (Pike, 2011). During the cold war Denmark had fast attack crafts and submarines with the effect of a fleet in being, but with powerful units as mobile missile batteries it would be possible to regain that effect to protect Bornholm and the Danish coastlines.

Conclusion - Considerations for Denmark

So, to answer the question on how Denmark should adjust its strategy and capabilities in the face of a new strategic challenge, I have reached the following conclusions.

With NATO's expansion with Finland and Sweden, NATO's first line of defence has moved further to the east. Denmark's traditional role in the Baltic Sea will be reduced, as the capability of Denmark only consists of area air defence frigates for the protection of a naval force. As the Russian Baltic Fleet still constitutes a threat in the Baltic Sea, it is evident that Sweden with its Submarine Forces will be a substantial contribution as one of NATO's means of deterrence in the Baltic.

As a small Navy, and a small state, Denmark must consider whether the strategy should primarily be to secure Bornholm, the Danish Straits, Kattegat, Skagerrak, North Atlantic and Arctic. The Danish straits are of great geopolitical importance to NATO. Hence, the Danish focus should be to prioritize the protection of the Danish straits and Denmark in all. By controlling and defending the Danish straits, NATO can restrict the Russian Naval Forces freedom of manoeuvre to and from the Baltic.

As for the protection of the Danish straits, Denmark must consider how to look at the old conventions and to maintain control and make sure the conventions are not violated, there must be a clear understanding of intervention and consequences if a hostile vessel violates the conventions for passage.

To face the threats of today, Denmark has several areas to consider in the maritime domain. Sovereignty enforcement in the Arctic area, at the Faroe Islands, Danish straits, and territorial waters of Denmark, and in the Baltic Sea around Bornholm. The geopolitical position Denmark holds, as well as the membership in NATO, assigns obligations to the country. With the frigates upgraded with ballistic missile defence and early warning radars, it would be possible to defeat ballistic missiles launched from Kaliningrad when positioned in the North Atlantic. To protect the critical underwater infrastructure, it would be necessary to use sensors for surveillance. That will release capabilities to other areas. Another way to free up naval capabilities could be the mobile coastal missile batteries which as well could deter the enemy from attack, constituting a fleet in being.

Bibliography

Lucas, Edward , et al. 2023. Sea Change: Nordic-Baltic Security in a New Era. *CEPA*. [Online] September 28, 2023. [Cited: October 3, 2023.] <https://cepa.org/comprehensive-reports/sea-change-nordic-baltic-security-in-a-new-era/>.

Asmussen, Birgitte Skovlund. 2023. Ruslands ambassade forsøgte ifølge Udenrigsministeriet at få efterretningsofficerer ansat: Tvinges nu til at reducere staben. [Russia's embassy, according to the Foreign Ministry, tried to hire intelligence officers: Now forced to reduce staff]. *DR*. [Online] September 1, 2023. [Cited: October 12, 2023.] <https://www.dr.dk/nyheder/seneste/udenrigsministeriet-der-skal-vaere-faerre-medarbejdere-paa-den-russiske-ambassade#:~:text=If%C3%B8lge%20den%20seneste%20liste%20fra%20Udenrigs ministeriet%20er%20der,bemandingen%20p%C3%A5%20ambassaden%20i%20K%C3%B8benhavn%20>.

Center for Cyber Security. 2023. The cyber threat against Denmark 2023. *Center for Cyber Security*. [Online] May 1, 2023. [Cited: October 12, 2023.] <https://www.cfcs.dk/globalassets/cfcs/dokumenter/trusselsvurderinger/en/the-cyber-threat-against-denmark-2023.pdf>.

Christensen, Andreas. 2000. Krigsskibes ret til gennemsejling af de danske stræder. [The right of warships to transit through the Danish straits]. *Horten Advokatpartnerselskab*. [Online] 2000. [Cited: October 12, 2023.] <https://www.horten.dk/~media/artikler/krigsskibes-ret-til-gennemsejling-af-de-danske-strder.pdf>.

Cooban, Anne. 2023. Suspected sabotage shuts another European gas pipeline. Here's what you need to know. *CNN*. [Online] October 11, 2023. [Cited: October 11, 2023.] <https://edition.cnn.com/2023/10/11/energy/baltic-pipeline-explainer/index.html>.

Danish Defence Intelligence Service and Police Intelligence Service. 2022. Truslen fra russisk paavirkning mod det kommende folketingsvalg. [The threat of Russian influence on the upcoming general election]. *Politiets Efterretningstjeneste*. [Online] 2022. [Cited: October 11, 2023.] <https://pet.dk/-/media/mediefiler/pet/dokumenter/analyser-og-vurderinger/truslen-fra-russisk-paavirkning-af-det-kommende-folketingsvalg.pdf>.

Danish Ministry of Defence, MoD. 2022. Danmark forstærker NATO-styrker med fregat og fire kampfly. [Denmark reinforces NATO forces with frigate and four fighter jets]. *FMN*. [Online] January 10, 2022. [Cited: October 11, 2023.] <https://www.fmn.dk/da/nyheder/2022/danmark-forstarker-nato-styrker-med-fregat-og-fire-kampfly/>.

—. 2004. Forsvarsforlig 2005-2009. [Defence Agreement 2005-2009]. *Forsvarsministeriet*. [Online] June 10, 2004. [Cited: October 11, 2023.] <https://www.fmn.dk/globalassets/fmn/dokumenter/forlig/-forsvarsforlig-2005-2009-inkl-bilag-.pdf>.

FMN. 2023. Forsvarsordførerne orienteret om kritisk NATO-rapport. [Defence spokesmen briefed on critical NATO report]. *FMN*. [Online] January 25, 2023. [Cited: October 13, 2023.] <https://www.fmn.dk/da/nyheder/2023/forsvarsordforerne-orienteret-om-kritisk-nato-rapport/>.

Folketinget. Year unknown. Grundloven og det danske demokrati. [The Constitution and Danish democracy]. *Folketinget*. [Online] Year unknown. [Cited: October 11, 2023.] <https://www.ft.dk/da/folkestyret/grundloven-og-folkestyret/grundloven-og-det-danske-demokrati>.

Frigaard, Anders Melchior. 2022. Russisk krigsskib krænkede dansk farvand to gange: 'Et forsøg på at intimidere Danmark' [Russian warship violated Danish waters twice: 'An attempt to intimidate Denmark']. *DR*. [Online] June 17, 2022. [Cited: October 3, 2023.] <https://www.dr.dk/nyheder/indland/russisk-krigsskib-kraenkede-dansk-farvand-gange-et-forsoeg-paa-intimidere-danmark>.

Ghaedi, Monir. 2022. Could Turkey close its waterway to the Russian navy? *DW - Made for minds*. [Online] February 28, 2022. [Cited: 10 5, 2023.] <https://www.dw.com/en/could-turkey-close-the-bosporus-to-the-russian-navy/a-60948124>.

Helsinki-Komité, Den Danske. Year unknown. Helsinki Principper [Helsinki Principles]. *Den Danske Helsinki-Komité*. [Online] Year unknown. [Cited: October 11, 2023.] <https://helsinkicommittee.dk/helsinki-principper/>.

Kriseinformation.dk. 2023. Denmark's contribution to support for Ukraine. *Kriseinformation.dk. National Communication Center in the Ministry of Foreign Affairs*. [Online] October 6, 2023. [Cited: October 11, 2023.] <https://en.kriseinformation.dk/war/denmarks-response/donations>.

Kristensen, Kristian Søby and Byrjalsen, Niels . 2022. Efter freden - Ukrainekrigens betydning for dansk og europæisk sikkerhed. [After the peace -The significance of the Ukraine war for Danish and European security]. *University of Copenhagen - Centre for Military Studies*. [Online] June 23, 2022. [Cited: October 2, 2023.] https://cms.polsci.ku.dk/publikationer/efter-freden/download-rapport/CMS-rapport_2022_4_-_Efter_freden_-_Ukrainekrigens_betydning_for_dansk_og_europ_isk_sikkerhed.pdf.

NATO. Year unknown. MY COUNTRY AND NATO. *NATO*. [Online] Year unknown. [Cited: October 10, 2023.] https://www.nato.int/cps/en/natohq/declassified_162357.htm.

—. 2023. Resilience, civil preparedness and Article 3. *NATO*. [Online] August 2, 2023. [Cited: October 11, 2023.] https://www.nato.int/cps/en/natohq/topics_132722.htm.

NORDEFECO. 2023. About NORDEFECO. *NORDEFECO*. [Online] 2023. [Cited: October 4, 2023.] <https://www.nordefco.org/the-basics-about-nordefco>.

Nordenman, Magnus. 2018. Issue Brief - Maritime Defense for the Baltic States. *Atlantic Council*. [Online] February 2018. [Cited: October 12, 2023.] https://www.atlanticcouncil.org/wp-content/uploads/2018/02/Baltic_States_Maritime_Defence_WEB.pdf.

Pesu, Dr Matti. 2023. Logical but unexpected: Witnessing Finland's path to NATO from a close distance. *NATO*. [Online] August 30, 2023. [Cited: October 11, 2023.] <https://www.nato.int/docu/review/articles/2023/08/30/logical-but-unexpected-witnessing-finlands-path-to-nato-from-a-close-distance/index.html>.

Pike, John. 2011. Military - Fleet in being. *Global Security*. [Online] July 5, 2011. [Cited: October <https://www.globalsecurity.org/military/ops/fleet-in-being.htm>, 2023.]

—. 2021. Montreux Convention 1936. *Global Security.org*. [Online] December 15, 2021. [Cited: October 2, 2023.] <https://www.globalsecurity.org/military/world/naval-arms-control-1936.htm>.

United Nations. 1958. Convention on the Territorial Sea and the Contiguous Zone 1958. *United Nations*. [Online] April 29, 1958. [Cited: October 12, 2023.] https://legal.un.org/ilc/texts/instruments/english/conventions/8_1_1958_territorial_sea.pdf.

Westersø, Rikke Struck. 2022. Danmark udviser 15 russiske diplomater for spionage. [Denmark expels 15 Russian diplomats for espionage]. *TV2*. [Online] April 5, 2022. [Cited: October 11, 2023.] <https://nyheder.tv2.dk/politik/2022-04-05-danmark-udviser-15-russiske-diplomater-for-spionage>.

Williams, Ian. 2017. The Russia – NATO A2AD Environment. *MissileThreat*. [Online] January 3, 2017. [Cited: 10 21, 2023.] <https://missilethreat.csis.org/russia-nato-a2ad-environment/>.

BRIEFING NOTE FOR THE ARGUMENTATIVE ESSAY PRESENTATION PANEL

“Danish strategic challenges in the Baltic Sea after NATO’s expansion with Finland and Sweden”

Aim

To argue that Denmark must adjust its strategy and capabilities in the face of a new strategic challenge.

Background / Framing the Problem

Denmark has several challenges as it is a small state but a large realm and must prioritize the capabilities to protect the Straits, Bornholm, and critical underwater infrastructure as well as protecting Danish sovereignty in the Arctic and the Faroe Islands. Every passage from the Baltic Sea to the North Sea or the North Atlantic is passing through the Danish straits. Since the beginning of the war in Ukraine, the security situation in the Baltic Sea, has changed significantly and both Finland and Sweden applied for NATO-membership. This essay will argue that Denmark must adjust its strategy and capabilities in the face of a new strategic challenge.

Discussion

The main argument for this essay is, that with Finland and Sweden joining NATO, Denmark and NATO must rethink its strategy in the Baltic Sea. The Danish Navy has limited capacity for coastal operations and needs capabilities for anti-submarine operations. It is therefore important, that Denmark and its alliance partners cooperates in defining what is needed to survey and defend the Baltic Sea area in all its dimensions. Denmark must, as well, prioritize protection of Danish straits, critical infrastructure, enforcement of sovereignty around Faroe Islands and the Arctic area. It is necessary to look at the conventions of passage of the straits to assess a possible violation as well as to look at Russian capabilities and the threats they represent.

Conclusion and Recommendations

NATO’s first line of defence has moved further to the east. The Danish straits are of great geopolitical importance to NATO. The Danish challenges are the protection of the Danish straits and Denmark in all. By controlling the Danish straits, NATO can restrict the Russian freedom of manoeuvre into and out of the Baltic. A clear understanding of intervention and consequences if a hostile vessel violates the conventions for passage is needed. To protect against ballistic missiles, the frigates must be upgraded with ballistic missile defence and early warning radars. To protect the critical underwater infrastructure, it would be necessary to use sensors for surveillance.

Prepared by: MCPO Jane Andersen
Supervisor: Dr. Viljar Veebel
Date prepared: 26th November 2023