Polish-Ukrainian military industry cooperation.

The rising military industry power?

FUNDACJA IM. KAZIMIERZA PUŁASKIEGO

PUŁASKI
REPORT

Polish-Ukrainian military industry cooperation.

The rising military industry power?

Authors

Bartłomiej Kucharski

Dariusz Materniak

Paulina Zamelek

Andrzej Kozłowski

Editor

Andrzej Kozłowski

Wydawca: Fundacja im. Kazimierza Pułaskiego

ul. Oleandrów 6, 00-629 Warszawa

www.pulaski.pl

Warszawa 2023

Table of Contents

Introduction

The large-scale Russian invasion of Ukraine at the beginning of 2022 has surprised many experts and is a consistent, heavy reminder to the European people that war in Europe is not a matter of the past. The invasion also brought significant changes in various areas of the worldwide security landscape. It started a new wave of military procurements and initiatives: repairing damaged military equipment and providing ammunition and other supplies needed for the contemporary battlefield. These factors have led to the reinvigoration of the military industry worldwide.

Both sides of the war are consistently searching all over the world for new military equipment, but this arms race has affected other countries as well. NATO members have increased defence spending and engaged in buying and producing new military equipment. One of the countries significantly active in this area is Poland, which decided to ramp up its defence spending to 4% of its GDP in 2023. Poland is also the main military hub for weapon deliveries to Ukraine, with the Rzeszów airport playing a leading role in this dimension. While the Polish Armed Forces have relied on post-soviet equipment in the past, they have engaged in an extensive transformation process to match Western standards and equipment. Thus, these factors make military cooperation between Poland and Ukraine a natural initiative. Despite this, it is not easy and there are many inherited challenges, but also opportunities for such cooperation.

Our report intends to find out the fields of potential cooperation, identify barriers and challenges, and provide recommendations on how to overcome them. It will also show how the Polish industry and security apparatus may use the Ukrainian war experience to improve their military products, as well as build common projects both in the short-term and long-term perspective. Lastly, our report will try to answer the question about the feasibility and profitability of any form of Polish-Ukrainian military collaboration.

Main research questions:

- What are the capabilities and strong/weak points of the Ukrainian and Polish military industries?

- What are the main barriers and challenges for the cooperation between the Ukrainian-Polish military industry and how do we overcome them?

- How can the Polish and Ukrainian industries capitalise from cooperation with each other?

- How to protect the possible cooperation between Polish and Ukrainian industries against hostile activities in the kinetic and cyber warfare domains?

- What are the short-term and long-term projects both countries can engage in?

- Is Polish-Ukrainian military company cooperation feasible?

The report consists of fourth chapters:

1. Polish and Ukrainian defence industry – characteristic
2. Potential financing sources for Polish-Ukrainian military projects
3. Potential areas of cooperation between Polish and Ukrainian arms companies
4. Security of the Polish-Ukrainian military cooperation

The first chapter describes the main characteristics of the Polish and Ukrainian military industries, enumerating the main military companies and research institutes and identifying strengths and weaknesses, as well as examining the impact of the 2022 war on the Ukrainian defence industry. Not to mention, the many similarities between the Ukrainian and Polish defence industries, including common areas of cooperation, which are good signals for the future.

Despite this, military cooperation needs financial resources, and thus Chapter Two will analyse the potential sources. It will look at different EU funds located within Permanent Structured Cooperation (PESCO) and other initiatives, which can be used in the area of military cooperation between Poland and Ukraine. What is more, NATO financial tools will also be analysed. The chapter ends with the possible consequences for Poland and Ukraine in the scope of the military cooperation between the two countries.

The third chapter focuses primarily on the potential areas of cooperation between Polish and Ukrainian arms companies. It identifies munitions such as tanks and infantry fighting vehicles, artillery, drones, small arms, as potential resources and other possible fields of cooperation by looking at past cases and recommending further projects. The chapter will also identify the main barriers and challenges ahead, in particular the role of the war and the still existing corruption and bureaucracy in Ukraine.

The last chapter stresses that any Polish-Ukrainian military cooperation entities will be susceptible to Russian hostile activities. Analysing the historical precedents, the chapter will present past sabotage actions and cyberattacks aimed at the military industry, which were done by both Russians and other hostile third parties. Based on precedents, the chapter will depict potential scenarios of attacks and propose a set of measures to minimise the risk of a success in such scenarios.

The Polish-Ukrainian military industry cooperation is a vital element of any collaboration between the two countries. It is a big chance both for Ukraine and Poland to transform the experience of war into effective cooperation in military areas, which will not only enhance security in Europe but together will also create a strong player in the military industry .

Leopard 2A5

Source: U.S Army Kevin S. Abel, Wikimedia Commons, CC0

1

Polish and Ukrainian defence industry - characteristics

Bartłomiej Kucharski

1.1 PDI – general characteristics

The Polish defence (armaments) industry was entirely inherited by the Republic of Poland (Third Republic) from the People's Republic of Poland, although the history of some plants dates back to the interwar period. In 1989, it was technically and technologically lagging behind its Western competitors in most respects, but this situation has improved in some areas over time. The defence industry as a whole consists of dozens of enterprises working for the Polish Armed Forces, other Polish uniformed formations (Police, Border Guard, etc.) and foreign customers. The defence industry is treated in contemporary politics, at least theoretically, as one of the elements of state security, providing equipment, armaments, ammunition, and maintenance and training services to recipients, which means primarily the domestic armed forces. Prior to the 1989 political transition, the armaments industry was wholly owned by the Polish state (PRL). Over time, some plants were privatised, some were liquidated altogether, and most underwent some form of restructuring and downsizing. This was related to the reduction in the size of the Polish Armed Forces (formerly the Polish People's Republic's Armed Forces) and the long-lasting economic crisis, stretching in fact from the late 1970s, which permanently delayed the implementation of successive modernisation plans. The situation of the Polish defence industry began to improve after joining NATO and later the European Union, with expanded access to foreign technologies, sub-suppliers of modern components and semi-finished products, and an improvement in the country's economic situation. The latter, along with first the war in Ukraine in 2014-15 and later the full-scale Russian invasion of Ukraine in early 2022, allowed for a significant increase in arms purchases, including in the Polish defence industry.

Polska Grupa Zbrojeniowa S.A.

The largest Polish defence company is Polska Grupa Zbrojeniowa S.A. (Polish Armaments Group). It is a capital group, not a conglomerate in the Western sense of the word (such as Rheinmetall AG, Lockheed Martin, Hanhwa Group, Leonardo, etc.), and as a result the group's management has limited influence on the operation of its constituent State Treasury Companies (Polish SSPs). The PGZ website reads:

"PGZ is a manufacturer of innovative systems and solutions used by the Polish Armed Forces and allied formations. The group's offer includes: modern radar and radiolocation systems, rifles, optoelectronics, wheeled armoured personnel carriers, barrel artillery, unmanned air systems and battlefield management systems. Our products are based on Polish technological thought and cooperation with world leaders in the defence sector. They are developed and manufactured under the supervision of experienced engineers, designers and specialists. Polska Grupa Zbrojeniowa is the main industrial partner of the Plan for Technical Modernization of the Polish Armed Forces, conducted by the Ministry of Defence. We cooperate with the world's largest companies in the arms industry and participate, among other things, in the program to build a medium-range anti-aircraft and anti-missile defence system. We use the technologies and competencies acquired in this way to further develop the Group's potential."[1]

PGZ S.A. is made up of 31 companies. The Group is divided into divisions, called Domains (internal working groups, working in mutually similar areas of activity). These are, respectively:

PGZ S.A. Land Domain, bringing together the companies: Autosan sp. z o.o., Zakłady Mechaniczne "Bumar - Łabędy" S.A., Huta Stalowa Wola S.A., Jelcz sp. z o.o., Ośrodek Badawczo-Rozwojowy Urządzeń Mechanicznych "OBRUM" sp. z o.o., Rosomak S.A., Stomil-Poznań S.A., Zakład Mechaniczny "Bumar-Mikulczyce" S.A. and Wojskowe Zakłady Motoryzacyjne S.A. In time, they are also expected to be joined by H.Cegielski-Poznan S.A., which was announced to be incorporated into PGZ S.A. in late August 2022. These companies are primarily involved in the production and servicing of military vehicles (and their components), including: trucks, wheeled armoured personnel carriers, self-propelled guns, etc. These plants are also involved in the servicing and modernisation of Leopard 2 tanks purchased in Germany and other ventures. In the future, this activity will continue and be expanded, among other things, due to planned orders, in particular: the K2PL basic tank programme (about 500 tanks and 200 specialised vehicles will be built in Poland, for the rest the PPO will participate in their production, service and modernisation), infantry fighting vehicle programmes (more than 1,400 lighter Borsuk and several hundred heavier vehicles, ZSSW-30 turret), artillery programmes (chassis and other components of Polish systems GMLRS/ATACMS, K239PL, K9PL, Langusta 2/3, Rak, artillery ammunition vehicles, etc.), the Waran programme (a 4x4 multipurpose armoured vehicle as a carrier in many other programmes) and others.

The arms and ammunition domain includes companies: Bydgoskie Zakłady Elektromechaniczne "Belma" S.A., CENZIN Sp. z o.o., Zakłady metalowe "Dezamet" S.A., Fabryka Broni "Łucznik"-Radom sp. z o.o., Przedsiębior-

M120 Rak **Source: PW2, Wikimedia Commons, CC3**

WLR 100 Liwiec **Source: AlfvanBeem, Wikimedia Commons, CC0**

stwo Sprzętu Ochronnego "Maskpol" S.A, Mesko S.A., Zakłady Chemiczne "Nitro-Chem" S.A., PCO S.A., Zakłady Mechaniczne "Tarnów" S.A., Wojskowe Zakłady Uzbrojenia S.A. and Zakład Produkcji Specjalnej "Gamrat". This Domain is much more diversified, as it includes both manufacturers of ammunition and its components (Dezamet, Nitro-Chem, Gamrat), as well as producers of armaments "Łucznik", ZM "Tarnów") or subassemblies for other companies (PCO) or uniforms and equipment (Maskpol). These companies are involved in the production of, among other things, ammunition of various types and calibres, manufacture of small arms, production of helmets, uniforms, optoelectronic systems, mines, etc. CENZIN, on the other hand, is not engaged in production, but in foreign trade. These companies are key to the following programmes: small arms (MSBS Grot, kbw), anti-tank (Pirat), ammunition (APR-120 and APR-155 precision ammunition, other types of ammunition), individual equipment (Tytan) and others.

The C4ISR (electronics, information technology and cybertechnology) domain includes companies: Ośrodek Badawczo-Rozwojowy Centrum Techniki Morskiej S.A., Pit-Radwar S.A., Wojskowe Zakłady Elektroniczne S.A., Wojskowe Zakłady Łączności No. 1 S.A., Wojskowe Zakłady Łączności No. 2 S.A. and Zurad Sp. z o.o.. They are engaged in the production of radiolocation stations, communications systems, radio-electronic warfare systems and other key solutions on the modern battlefield. They play an important role in the implementation of programmes related to air defense, such as Vistula, Narew, Pilica+ and others. Zurad, on the other hand, produces solutions related to traffic management (such as speed cameras).

The aviation domain brings together the following companies: Wojskowe Centralne Biuro Konstrukcyjno-Technologiczne S.A., Wojskowe Zakłady Lotnicze No. 1 S.A., Wojskowe Zakłady Lotnicze No. 2 S.A. and Wytwórnia Sprzętu Komunikacyjnego "PZL-Kalisz" S.A.. These companies are involved in the aviation industry in the broadest sense, manufacturing auxiliary equipment used at airports, manufacturing and servicing unmanned aircraft, servicing manned aircraft used by the Polish Armed Forces, etc. They are involved, among other things, in servicing Polish F-16s, helicopters, but also in work for the civilian market.

The Maritime Domain consists of PGZ Stocznia Wojenna sp. z o.o., whose main area of involvement is the Miecznik programme, which includes the delivery of 3 missile frigates for the Polish Navy over the next few years.

PGZ Naval Shipyard **Source: Apienkos, Wikimedia Commons, CC4**

WB Group Headquarters

Source: Andrzej Błaszczak, Wikimedia Commons, CC4

The companies that make up PGZ S.A. play a leading role in most of the programmes carried out for the Polish Armed Forces. In some, such as "off-the-shelf" purchases (e.g., M1 Abrams tanks), they play a supporting role (in the case of Abrams, they are likely to be fully or partially responsible for servicing these tanks). In only a few do they play no role or only a negligible role (the F-35A purchase), although this may change over time.

1.2 Private businesses

Poland's defence industry does not consist exclusively of state-owned companies. There are also private companies, created by privatising formerly state-owned enterprises or by creating new companies from scratch. These are companies representing various branches of defence production. The WB Group's member companies, such as WB Electronics, WBE Technologies, Arex, Flytronic and Radmor, seem to be developing particularly rapidly. The three core business areas of WB Group companies are communications systems (radios, battlefield management systems), fire control systems (Topaz artillery fire control and communications system, elements of the ZSSW-30 turret fire control and communications system) and unmanned aerial vehicles (FlyEye, Warmate, Warmate 2 - including circulating munitions versions). WB Group is present in many programmes carried out for the Polish Armed Forces, such as Borsuk, Gladius and virtually all artillery programmes. The company also carries out numerous foreign orders, including for the Armed Forces of Ukraine or the United States of America (independently and in cooperation with local industry).

Interesting solutions in the field of communication systems are also offered by private companies such as Teldat (BMS/HMS Jasmin system), KenBIT (BMS Hektor, ship communication systems) or Transbit (radio beacons, radios). Unmanned aircraft (including circulating munitions) are offered by MSP and Asseco Poland, while APS offers a powerful system for fighting them (SKYCtrl). Works11 or Niewiadów offer wide assortments of various weapon systems and services, also imported in the case of the former company. Gdańska Stocznia Remontowa, which is responsible

ORP Kormoran

Source: Tomasz Grotnik, Polish Ministry of National Defence, CC3

Piorun Anti-Aircraft Missile Source: Ministerstwo Obrony Narodowej, Wikimedia Commons, CC3

for the construction and delivery of a series of modern Kormoran II-type mine destroyers for the Polish Navy, has had great success. Polish private companies are also involved in the development and production of combat vehicles. These include AMZ Kutno and Mista. The Kutno-based company is known for developing and producing a number of 4x4 armoured vehicles of the MRAP class (Zubr being the carrier of the Poprad anti-aircraft system, the Tur series), as well as wheeled armoured personnel carriers: Bobr (offered to the Polish army as part of the programme to purchase a reconnaissance vehicle codenamed Kleszcz) and Hipopotam (a heavy, large 8x8 floating armoured carrier). Mista, in turn, mass-produces, among other things, Oncilla light wheeled transporters, which are a Polonised variant of the Ukrainian Dozor-B vehicle. Unarmoured vehicles are produced or adapted by companies such as Auto Podlasie (manufacturer of the highly successful AERO for aero mobile forces and the RECON light armoured vehicle) and Szczesniak Special Vehicles (with a wide range of rescue and firefighting vehicles on IVECO or Scania chassis). An interesting institution is CRW Telesystem-Mesko sp. z o.o., which is a key partner of PGZ S.A. companies in some projects, such as the Grom and Piorun anti-aircraft systems, the Pirat anti-tank system, etc. There are also a number of smaller companies engaged in the production of armament components or even whole weapons (mostly small arms), arms trading, refurbishing, etc.

Private companies are not as big players in the market as PGZ S.A., but nevertheless offer many interesting and often completely modern solutions. This allows them to be present in foreign markets, where - at least some of them - are slowly gaining a relatively good position. Nevertheless, the solutions of some private companies are also present in the Polish Armed Forces, while the increase in arms purchases after the outbreak of war in Ukraine also results in an increase in the order portfolio of at least some private defence companies.

1.3 Foreign companies manufacturing in Poland

Several major Western corporations have their own plants in Poland. These are mostly former State Treasury Aviation Companies, Polskie Zakłady Lotnicze. The best known are PZL-e: Świdnik, Mielec and Okęcie. The first of the plants, PZL Świdnik, is owned by the Italian company Leonardo. It participates in the servicing of formerly manufactured Polish helicopters (such as the W-3 Sokół family) and in the production of modern helicopters for the parent concern. Thus, it participates in the supply of Leonardo-produced helicopters to the Polish Armed Forces (AW101, AW149). The second company, PZL Mielec, is owned by Lockheed Martin (through Sikorsky Aircraft Corporation) and produces Black Hawk helicopters in the S-70i version, devoid of sensitive technologies owned by the US government. These helicopters are also supplied to the Polish army and beyond - the Police also use them. They are also manufactured for export. The last company, PZL Okęcie, is now part of the Airbus concern and is called Airbus Poland S.A. It carries out orders related to, among other things, the production of CASA C-295M transport aircraft. The American company Pratt & Whitney (part of the Raytheon concern), which manufactures aircraft engines, also has its plants in Poland (in Kalisz and Rzeszów).

S-70 Black Hawk Source: Jakub Hałun, Wikimedia Commons, CC4

In addition, according to unconfirmed information, in connection with large foreign purchases, some manufacturers would be opening plants in Poland. This applies in particular to the US conglomerate General Dynamics Land Systems (manufacturer of the Abrams tank) and South Korea's Hanwha Aerospace (manufacturer of the K9 and K239, among others). Subsidiaries of the corporations could handle, among other things, servicing of armaments purchased by Poland, although this would mean creating competition for Polish industry, in particular for PGZ S.A.

1.4 Along with production: sub-suppliers and research institutes

There are a number of plants and institutions supporting armaments production. Leading the way, of course, is the metallurgical (iron and steel) industry, such as Huta Stali Jakościowych. There are plants supplying various small components, semi-finished products, etc., which are sub-suppliers to the armaments industry, among others. Their products receive little media coverage, but are important because of their significance to the operation of the final products of armaments plants. New companies are constantly emerging (or existing ones are expanding into the armaments sector), such as Jetpol, a manufacturer of miniature jet engines with the possibility of being used to propel, for example, cruise missiles. With the growing importance of energy storage (batteries powering individual soldier equipment, batteries for electric and hybrid vehicles), the importance of the particularly strong but often overlooked industry of Polish battery and battery manufacturers, who are among the strongest on the market, may increase.

Numerous scientific institutions also cooperate with the defence industry. Some of them are grouped under the Lukasiewicz Research Network. This network carries out a range of work related to, among other things, the defence industry, including: unmanned, aerospace, composite, manufacturing technologies, etc. The defence industry also cooperates with military research institutes, such as WITU, WIŁ, WIChiR, WITI, WITPiS, etc. These institutions sometimes attempt to develop solutions for new types and kinds of weapons on their own. An example is the Moskit anti-tank guided missile, developed by WITU, which may in time go into production. A similar function is fulfilled by some universities, including the Military Academy of Technology (and military universities more broadly) or the Gdansk University of Technology (which has a great deal of merit related to work on anti-mine systems) or the Silesian University of Technology (which cooperates with Silesian armoured centres).

Łukasiewicz Research Network Source: Mateusz Gdynia, Wikimedia Commons, CC4

1.5 PDI – strengths and weaknesses

Every organisational unit, or collective, such as the defence industry is characterised by a certain specialisation. The Polish defence industry as a whole, as well as individual business entities, have certain competencies, production capacities, proprietary solutions developed over the years or acquired licenses, and so on. Similarly, there are certain gaps and shortages in terms of competencies.

Strengths of PDI

The strengths of the Polish defence industry include particularly large production capacities in certain areas. This is especially true in those areas in which investments have been made over the past several years. Thus, Polish industry has built up and has competence in the development and production of armoured vehicles of various types and classes, their components, armaments, etc. It has also built up quite extensive capabilities related to the development of artillery and anti-aircraft missiles, laser-guided precision-guided artillery munitions, communications systems, drones, etc. These capabilities, as well as production capacity, will grow over the course of the next major modernisation programmes, where the Polish defence industry is a major implementer or sub-supplier (though limited for now). Advantages also include the relatively high quality of products, which often do not deviate in quality and parameters from today's best designs. The Polish defence industry also acts as a sub-supplier for foreign companies, including the F-35/JSF programme, the NSM programme or, in the future, Type 31 frigates. Some of these competencies have been obtained through offsets or licenses. It should be expected that the relatively large investments anticipated in the coming years will exacerbate the trend of expanding production capabilities, especially for a wide range of armaments for Land Forces. This is because they mean, among other things, relatively large investments in production infrastructure, training of crews, hiring of new employees

F-35 Source: Wikimedia Commons, CC4

at various levels, etc. This also applies to the implementation of completely new competencies, such as the development and production of anti-drone systems. In turn, the Polish branches of foreign concerns provide an important complement to the production competencies (although not always scientific) of their parent companies.

Weaknesses of PDI

The Polish defence industry's fundamental weakness is its structural character. It results, among other things, from the lack of a holding law, which does not allow the consolidation of PGZ S.A. into a single strong armaments conglomerate on the model of the large Western corporations, with a unified management and board of directors setting the general directions and goals of the group, coordinating cooperation between companies and capable of forcing behaviour that does not generate problems for the other members of the group. The treatment of state-owned companies (including Polish defence industry) as political spoils by politicians has similar effects. The positions of CEOs or board members mean high salaries, so after the elections they become a gluttonous morsel for politicians of the winning party, and often even during the term of office the people holding the position are replaced. This makes it impossible (or at least difficult) to maintain organisational continuity to gain relevant experience in project and company management, etc. This significantly limits the effectiveness of the management of Poland's main armaments company. A similar problem is the weakness of private companies, much smaller than PGZ S.A. - so they cannot fully compete effectively with the state-owned entity, especially since politicians often prefer the products of those companies they control. Sometimes state and private companies cooperate with each other, but unfortunately there are cases where, despite cooperation, two supposedly partner entities are able to operate to each other's detriment.

A similar character is the selection of armaments according to a political key on the basis of ad hoc needs. This occurred in the case of purchases of helicopters for the Polish Armed Forces, the purchase of two comparable types of basic tank instead of one (which further increases the cost of servicing the armed forces by introducing logistical chaos and reducing the so-called economies of scale of the order), etc. The development of the potential of the Polish armaments industry is also effectively limited by very small expenditures on research and development. Although they are mostly used quite effectively, the low outlays, many times lower than in many European countries, handicap the development of the defence industry, which requires the use of modern technical and technological solutions.

Bayraktar TB2 Source: Bayhaluk, Wikimedia Commons, CC4

At the same time, Polish politicians are able to make decisions on the purchase of foreign weapons systems, which could be developed by domestic entities without much hindrance, if only these entities had adequate resources. A good example is the purchase of Turkish Bayraktar TB2 UCAV, as there is nothing to prevent, for example, the WB Group or PGZ S.A. from developing domestic equivalents. The scale of necessary investments is also a significant problem - those announced, although large, are sometimes insufficient, as a result of years of neglect, resulting in technological backwardness sometimes counted in decades. A significant problem is also the dependence on foreign sub--suppliers in such key issues as the propulsion systems of armoured vehicles, certain elements of armaments (e.g. the Mk44S cannon which is the armament of the Rosomak Wheeled Armoured Vehicle), etc. This affects, among other things, the restriction of rights to export armaments to third markets, and requires spending significant sums on the purchase of components, which in turn translates into an outflow of funds from the Polish economy (e.g. in the case of the aforementioned Rosomak, but also, to a lesser extent, the Krab). Another factor limiting exports is the unfavourable state policy on arms and ammunition exports, including a complete lack of clear export support mechanisms. It is worth noting that many of the pathologies and problems plaguing the industry are in fact not directly troubles resulting from the situation of the company in question (management model, wrong decisions, etc.), but structural and institutional problems of the Polish state and the conscious choices of politicians.

KTO Rosomak Source: Robert Douglas, Michigan Army National Guard, CC0

1.6 Industry of UA – general characteristics

The Ukrainian armaments industry, like the Polish, is an industry inherited from a country with a different political, social and economic system, and in the case of Ukraine this is exacerbated by the fact that the current statehood of Ukraine was created as a result of the collapse of the USSR in 1991. Initially, the Ukrainian industry did not decline much, due to continued cooperation with the defence industry of Russia and Belarus (e.g. the Nota new generation tank programme). The situation began to deteriorate especially after 2000, with Ukraine's difficult political and economic situation. As the Ukrainian people, and in time its politicians, took a pro-Western course, Ukrainian industry was slowly hampered in its access to a network of sub-suppliers deployed in Russia (and to a lesser extent in Belarus, which maintained correct relations with its southern neighbour until 2022). This was facilitated by the fact that Ukrainian industry before 1991 was part of the USSR's war-industrial complex, whose various plants were spread throughout the communist empire. This problem became particularly evident after 2014, when Ukraine attempted to proceed with an export armour contract for Thailand, which was experiencing long delays due to obstructions from Russian sub-suppliers (exacerbated by the loss of Theodosia, home to license thermal camera manufacturer Thales Catherine). The same was true of ambitious aviation programmes (such as the Antonov An-70). In general, it can be assumed that Ukraine's defence industry - both state and private - shared the fate of the entire state and nation after 1991, while the last years of its functioning were particularly affected by the period of struggle for independence from the Russian Federation, when the industry had to operate under completely new conditions.

However, it should be mentioned that after 2014-15, Ukrainian-Russian industrial cooperation occasionally continued, not always legally. The poverty prevailing in Ukraine after the collapse of the USSR and the virtually permanent crisis meant that Ukraine's defence industry subsisted mainly on exports. This did not always involve the sale of new products (as it was the case of e.g. T-80UDs sold to Pakistan in the 1990s), a large role in providing funds for the functioning of the Ukrainian industry (and Ukraine in general) was played by the sale of armaments inherited from the USSR, exported especially in the 1990s in huge quantities and often beyond official control. Happily, this did not apply to nuclear weapons, which Ukraine gave away. Due to the outbreak (resumption) of war in February 2022, many of Ukraine's defence enterprises were destroyed, damaged or were in occupied territories, so the following will describe the pre-war status.

Ukroboronprom

The most important Ukrainian arms enterprise is the state corporation Ukroboronprom. The corporation's main tasks at the time of its establishment were to implement centralised supervisory activities, help utilise and develop the potential of companies, create and offer advanced products to markets, support their implementation into production, attract investors, develop marketing strategies, and develop foreign contacts. Naturally, the most important market for Ukraine's defence industry is the home market, although until 2014 the main source of income was exports of goods and services. Before the war, the conglomerate included more than 100 different enterprises in various industries, still originating from the Soviet Union's war-industrial complex. One of the company's best-known areas of activity was the maintenance, repair, modernisation and production of armoured vehicles. The Kharkiv Combines in particular specialised in this field, still in charge of developing and producing the best Soviet tanks (from the T-34 to the T-64, the T-80UD and fourth-generation tank projects, including those that continued after the collapse of the USSR) and their development versions (the T-84 BM Oplot).

T-80

Source: 93rd Mechanized Brigade of Ukrainian Ground Forces, CCO

Most important among them were the Malyshev Plant and the Morozov Design Bureau, also responsible in recent years for the production of the BTR-3 and BTR-4 wheeled armoured personnel carriers (modernized BTR-80) and the lighter Dozor-B (4x4), as well as the development of the BMP-U infantry fighting vehicle. Other important enterprises involved in the production or service of armoured weapons were the Zhytomyr plant (manufacturer of several types of manned or unmanned turrets), Kiev or Lviv, while among the cooperators were Fotoprivlad, the Izjum plant (both of which were responsible for components of fire control systems) or the Kharkiv plant producing TD-series engines (especially 3TD, 5TD, 6TD). Until 2014, the electro-optical plants in Feodosia in Crimea were of great importance. They were also known for interesting solutions for securing armoured vehicles, such as the Microtec Zasłon active vehicle protection system and the Nóż/Duplet reactive armour. Many of the plants incorporated into Ukroboronprom were involved in shipbuilding, although after 1991 they did not have many orders, while the Russian shipbuilding industry was the largest customer (which, incidentally, led, for example, to the delay of the Admiral Gorshkov-type missile frigate programme). The Nikolaev shipyard was once the only Soviet shipyard capable of building aircraft carriers, but due to a lack of orders it had already been put into bankruptcy before the war.

A number of Ukroboronprom enterprises are involved in the production of communications and radiolocation systems. These include Kharkiv's Proton plant, Odessa's Molniya plant, Kiev's Kvant institute and Zaporizhia's Radioprilad plant. During the Soviet era, they participated in the development and production of numerous anti-aircraft complexes (S-75, S-125, S-300), and after the collapse of the USSR in their modernisation and ensuring their efficiency. In addition, they supplied the Armed Forces of Ukraine with communications systems, radio-electronic warfare, etc. Of great importance, of course, is the munitions industry. It is capable of producing anti-aircraft system missiles (Wizar) or ammunition components (e.g., Impulse, Zirka). Particularly outstanding is the Łucz Construction Bureau, which is one of the proverbial pearls in the crown of Ukraine's defence industry. KB Łucz was capable of producing many different types of laser-guided anti-tank missiles (Korsar, Skif/Stugna, etc.), but also air-to-air missiles (UP-277), anti-aircraft missiles (RK-10), anti-ship missiles (the Neptune system, probably responsible for the destruction of the cruiser Moscow) or even ballistic missiles (the Grim-2 system) and precision-guided artillery munitions (152/155 mm Kwitnik missile, the Wilcha system).

A number of Ukroboronprom's constituent enterprises are active in aviation, including Zaporizhia's MiGremont plant, Lutsk's Motor plant (which produces RD-33 jet engines, including for export), as well as plants in Lviv, Kharkiv, Zhytomyr and other cities. Prior to the war, they were mainly concerned with ensuring the efficiency of Ukraine's relatively large air force, and on a small scale with modernising the aircraft fleet. For several years, some of the companies began research work related to unmanned aircraft (e.g., the Ukrinmash company). Among the biggest achievements at the time of Ukraine's independence are the KT-112 Kadet light helicopter and its armed version, the KT-112UD. Several separate companies headed by Spectechnoeksport handle the company's foreign trade.

BTR-4

Source: Artemis Dread, Wikimedia Commons, CC4

1.7 Aviation

Two aviation companies deserve separate discussion - Antonov (it is part of Ukroboronprom) and Motor Sich

R-360 Neptune **Source: VoidWanderer, Wikimedia Commons, CC4**

(privately owned before the war). Antonov's plant is responsible for the creation of many aircraft that are important to the history of world aviation, including the legendary (though destroyed at the beginning of the war) An-225 Miriya, An-124 Ruslan and others. After the collapse of the USSR, the plant continued to cooperate with Russian industry, including during the joint project of the An-70 medium military transport aircraft (the eastern equivalent of the A-400M Atlas). Due to Russia's sabotage of the project and the start of the conflict in 2014, the programme effectively collapsed. Based on the experience gained at Antonov, the An-77 (a heavy turbojet-powered transport aircraft) and An-188 (a slightly smaller turbojet-powered An-70) programmes were started. Due to lack of funds and time, their prototypes were not built. More fortunate was the smaller An-178, built in 4 examples (out of 24 ordered by Ukraine, Azerbaijan and Peru). The smaller aircraft, with a payload of 15-18 tons, can be considered the equivalent of the C-130 (albeit with turbojet propulsion). The outbreak of war also interrupted several civilian projects.

Motor Sich, on the other hand, is a private enterprise that manufactures various types of turbines, especially turboprop and turbojet engines. The company's offer includes more than a dozen models of engines of different power or thrust, possible for use in military and civilian machines of Eastern production (Tupolev, Yakovlev Mila or Antonov). An important achievement was the development several years ago of the MSB-2 Nadia helicopter, which is admittedly a modernised Soviet Mi-2, but the newer machine is made of much more modern materials and differs from the original in a number of design details. Motor Sich has several production facilities. Interestingly, both aerospace companies have their own airlines.

An-225 Mrija **Source: Mark Steven, Wikimedia Commons, CC3**

Antonov An-178 **Source: Vasiliy Koba, Wikimedia Commons, CC4**

1.8 Private businesses

Ukraine also has defence industry plants in private hands. Privately owned enterprises are engaged, as in Poland, in diverse activities. Among the most important enterprises are Ukrainian Armor, AutoKrAZ, Praktika and Kuznia na Rybalskie.

The first of the enterprises is engaged in adapting vehicle chassis plates in the market to carry specialised bodies, including in the form of light wheeled armoured personnel carriers. Major products include the Varta (a fairly large 4x4 light wheeled armoured personnel carrier/MRAP) and the Novator (a lighter 4x4 armoured vehicle). Both were mass-produced before the war, the former even in specialised variants (such as the carrier of the Polish-Ukrainian Sokił reconnaissance and strike system). Based on the lighter Novator variant, the Smereka light self-propelled mortar project was developed. The delivered vehicles were used by the Ukrainian Armed Forces during the 2022 fighting.

AutoKrAZ, in turn, is a manufacturer of trucks and derivative chassis for the installation of various applications. The plant's traditions date back to Soviet times. KrAZ's 4x4, 6x6 and 8x8 and larger chassis are used as specialised carriers for various artillery systems (especially rocket artillery, but also the 155mm self-propelled 2S22 Bogdan cannon howitzer, which is an independent development of the plant), radiolocation systems (such as the Amber-1800), engineering, logistics and other systems. KrAZ also supplies classic trucks, designed for passenger and cargo transport, such as the B6.2MEX, B12.2MEX, 5233BE models, truck tractors (e.g., 6510TE, 6443 models), etc. KrAZ has designed some interesting armoured vehicles, including the Kugar (4x4), the slightly larger Spartan (also 4x4) or the Hulk and Shrek/Shrek-M (also 4x4), weighing several tons each, the Fiona (6x6) or the heavy floating Hurricane (8x8). The company is the primary supplier of trucks and specialty carriers to the Ukrainian Armed Forces, with many models built after 1991.

PJSC Praktika is a unique company, as it was established only in 1993. It has been involved in defence production since 2009, when it developed its own 4x4 Kozak armoured vehicle. Over time, the range expanded to include other vehicles, such as the more modern Kozak 2, an armoured truck based on the KrAZ truck, several models of civilian off-road vehicles with added armour (including the Toyota Hilux, Land Rover Defen-

KrAZ-6446 **Source: Ministry of Defense of Ukraine, Wikimedia Commons, CC2**

Kozak-2M **Source: VoidWanderer, Wikimedia Commons, CC4**

der). The most interesting products, however, were wheeled armoured personnel carriers of the Otoman family, developed on the basis of the old Soviet BTR-60 transporter. Several variants were created in 6x6 and 8x8 layouts. Despite their vintage "ancestor," some prototypes used such technical innovations as LimpidArmor's omnidirectional observation system (it uses head-mounted displays). They did not manage to enter production, although the Otoman 3 was of interest to the Ukrainian Navy's Marine Corps. In all, the company has delivered more than 300 vehicles of various types to the Ukrainian Armed Forces, mainly the Kozak family.

The Rybalsky Forge, on the other hand, is a plant that originated in Kiev, but was a shipbuilding enterprise. The plant has been involved in the production of Project 1143M and MU small corvettes, Project 58150 and 58155 riverine armoured ships (Gyurza and Gyurza-M), Project Vespa small missile ships (construction has not formally begun) and other small warships (but also civilian). In addition to shipbuilding, the company is also involved in machine building and armament production, such as the UAG-40 automatic grenade launcher and the six-barrel 30mm anti-aircraft ship cannon. The company has also developed its own 4x4 Triton light wheeled armoured personnel carrier, developed based on components of the BTR-70 carrier.

A separate and interesting case is the Arej Engineering Group, based on a team of technicians working in 2014-15 for the Azov battalion's machinery park. The enterprise, working closely with Ukroboronprom's Kharkiv plant, was mainly engaged in the overhaul and modification of its armoured vehicles. Around 2016, the group's ambitions became high enough to undertake a proposal to develop new heavy armoured personnel carriers, AFV, and even a new-generation T-Rex tank. However, it ended up with unambitious prototypes based on solutions remembering the Soviet era.

1.9 Ukrainian defence industry - strengths and weaknesses

Like Poland's defence industry, Ukraine's industry before the outbreak of war had several areas in which it specialised and achieved great success. However, it also had significant skill shortages, exacerbated by the outbreak of war.

Strengths of the Ukrainian defence industry

The Ukrainian defence industry specialised before the outbreak of war in several areas. The first was its extensive experience in co-production, cooperation in development, and in the overhaul and modernisation of post-Soviet aircraft. This made it possible, despite limited resources, to create several interesting and promising designs, particularly those originating from the Antonov office. They could not only compete, but also be an excellent complement to more expensive Western-made aircraft, among which the lack of an intermediate-class transport aircraft between strategic transport aircraft (C-17A, C-5) and smaller aircraft (such as the A-400M or, especially, the even smaller C-390 and C-130) is clearly visible. Ambitions were high, as Ukrainian industry also had plans to build a wide range of unmanned aircraft, including heavy MALE class.

The second pillar of Ukrainian industry was the munitions industry, particularly concerning rocket munitions. During the first weeks of the war, the anti-tank guided missiles of the Barrier/Skif or Korsar family manufactured by KB Lucz formed the core of Ukrainian anti-tank defences and proved to be highly successful products, although perhaps less advanced than the top-attack, wire-guided missiles (Spike-MR/LR, MMP, etc.). Similarly, the Neptune anti-ship missiles, although introduced into service rather experimentally and just before the outbreak of war, probably had some success at the front (they are credited with destroying the large missile cruiser Moskva among other things). Before the outbreak of the war, Ukrainian industry managed to supply some batches of artillery barrelled precision-guided missiles Kwitnik and rocket-guided missiles Wilcha, and they too were used during combat, displaying considerable effectiveness.

There was not enough time to produce a batch of Grim-2 ballistic missiles, but they were considered sufficiently promising that the Kingdom of Saudi Arabia's army expressed interest in them (and not only in them, because also, for example, in Skifs, which Turkey is also likely to have bought), which seems to set a good reputation for Ukrainian products. In terms of vehicles, the Kharkiv centre has traditionally been of great importance, but not only. Although the Ukrainian armoured industry had its best years far behind it, attempts were slowly being made to rebuild its former potential, including attempts to Ukrainianise the T-84 tank (the version for Thailand dependent on Russian and Belarusian components), the production of mediocre but with some advantages wheeled armoured personnel carriers, or some very interesting, successful modernisations of old infantry fighting vehicles. Considerable significance in this context was the development and implementation into production of many types of manned and unmanned turrets, the installation of which on old chassis allowed to leapfrog the performance of the BMP-1 or BMP-2. An interesting case is the active shield protection system of the Zasłon, which, although did not enter into use in the Ukrainian army, was widely offered for export and found a buyer (Turkey), where the Aselsan company acquired a license for it (as Akkor Pulat) - it will be used there to shield Leopard 2 and Altay tanks.

Grom-2

Source: VoidWanderer, Wikimedia Commons, CC4

Weaknesses of the Ukrainian defence industry

Of course, not in every area of activity did the Ukrainian defence industry prosper. Especially after 2014, the negative consequences of dependence on Russian sub-suppliers made their presence known. While problems with Belarusian supplies, interestingly, did not exist until 2022, problems with Russian sub-suppliers arose relatively quickly, affecting, among other things, a delay of several years in the delivery of T-84 tanks to Thailand, and the subsequent cancellation of that country's further orders (which in total could have quadrupled to around 200 vehicles). Of course, this worked both ways (see: Russian Admiral Gorshkov-type frigates with Ukrainian engines) however, Russia, as the richer country, had fewer problems replacing Ukrainian subcontractors with others. This was compounded by the Russian Federation's illegal seizure of Crimea and the leading of an anti-Ukrainian rebellion (supported by the Kremlin, by the way) in Lugansk and Donetsk in 2014. Thus, a number of important arms companies were left outside the areas controlled by the legal authorities from Kiev, the loss of which further exacerbated the industry's problems.

T-84

Source: Wikimedia Commons, CC0

Organisational problems were also a significant concern. Permanent underfunding, corruption, and still strong Russian influence (as recently as 2022, Motor Sich chairman Vyacheslav Boguslayev was arrested on treason charges), caused a number of problems on the Ukrainian side. Many investments, although planned and paid for several years before the war, were not even started until the outbreak of the war (for example, a complex of spare parts warehouses for ground army vehicles). Perhaps the same source was the known problems with the quality of some products - Iraq, for example, abandoned a major contract for the purchase of BTR-4 wheeled armoured personnel carriers after the hulls of the first of 420 vehicles ordered appeared to crack in normal use. Similarly, the TD family's unconventional but potentially very interesting engines suffered a number of defects, despite decades of development. It seems that before the war, only the 5TD engine (in the 5TDF version), used in the T-64, was a fully mature product. The newer and more powerful 6TD (especially the 6TD-3 with 1,500 horsepower) appears to be still underdeveloped, as the older version was already complained about by the Pakistanis, who had been using T-80UDs powered by these engines for nearly 30 years (low inter-overhaul resource, high fuel burn). The smaller 3TD, intended to power some lighter vehicles, also seems not to have fully met expectations, as some modernisations or even production of new medium-weight vehicles have used engines from the German company Deutz.

Some problems, such as the issue of finding replacements for components of Russian origin, were not completely resolved until the outbreak of war. This is due to, among other things, underfunding, organisational problems (Russian influence, corruption still present) or lack of time to implement modified or completely new products.

1.2.0 Impact of 2022 war on Ukraine's defence industry

The full-scale Russian invasion of Ukraine in 2022 affected Ukraine's arms industry similarly, as well as the country as a whole. Unfortunately, negative trends prevailed. Many armaments companies were located in areas permanently or temporarily occupied by the aggressor. Already in 2014-15, due to the loss of Crimea and the territories of the pseudo-states in the east of Ukraine (the so-called Lugansk and Donetsk People's Republics), Ukroboronprom alone lost 11 enterprises, including the Donetsk Chemical Plant, the Lugansk Ammunition Plant or the Feodosia (Crimea) Optical Plant. After February 24, 2022, the problem worsened by leaps and bounds, as many plants were completely or partially destroyed. The Izjum Optical Plant was partially destroyed and looted after the Russians occupied the city. A similar fate befell many plants located in cities close to the front line, including Zaporizhzhya, Mariupol, Azov (the famous Azovstal metallurgical plant for its prolonged fighting), and especially Kharkiv, which until 2022 was one of the most important centres of the arms industry in Ukraine. Some of the plants' crews and movable assets probably managed to evacuate to the western part of Ukraine, but it should be remembered that the Russian bombardment affected virtually all of the country's territory, and plants further west also sustained some damage, paralysing or at least temporarily disorganising production and weakening Ukraine's defence and industrial potential.

Russian bombing of Mariupol Source: Ministry of Internal Affairs of Ukraine, Wikimedia Commons, CC4

The greater achievement is the maintenance of production or its resumption at some of the evacuated plants. For understandable reasons, there is little information available, but sometimes the Defence Ministry or the Ukrainian president provide isolated information on arms production at plants owned by Ukroboronprom or other Ukrainian enterprises. What is known, among other things, is the evacuation of part of the facilities of KB Łucz or some Kharkiv plants, but also Lviv repair plants.

Ukrainian industry has also retained some of its combat aircraft capability - for example, most, if not all, of the MiG-29 combat aircraft donated by Slovakia arrived in Ukraine by ground route as partially disassembled machines, while they were reassembled locally (perhaps in Lviv at the State Repair Plant). What's more, the situation of some plants is good enough to put brand new weapons systems into production. The AutoKrAZ plant, for example, announced the start of production of a 155mm self-propelled cannon howitzer on a Bogdan wheeled chassis, while Ukroboronprom announced in late 2022 the start of production of a long-range heavy circulating munition capable of delivering a 75kg warhead at a distance of up to 1,000 km. This means that despite Ukraine's war and Russian bombardment, Ukrainian industry has not only retained some of its competencies, but - presumably - also the ability to acquire new and develop existing ones, perhaps as part of the mobilisation of the economy.

The establishment of strategic partnerships with industries of Western countries supporting Ukraine is also not insignificant. Both sides have reported on a number of occasions that Ukrainian companies are launching production or overhaul of armaments for the Ukrainian Armed Forces outside Ukraine, usually in cooperation with local companies. It is known, for example, that production of mortar ammunition has been launched at a plant located on the territory of an undisclosed state, or that work on the overhaul of armaments for the Ukrainian Armed Forces is already underway or is planned in cooperation with Polish, Czech, Slovak, Lithuanian or Romanian industry. This means that, at least in part, the production of Ukrainian armaments, spare parts or ammunition is being reproduced outside Ukraine. This is a temporary state of affairs, as it is unofficially known that there are plans to reconstruct some destroyed plants (such as the Malyshev Factory), albeit in new locations, mostly in the western part of the country. There are also some proposals from the West for cooperation related to the possible production of modern armaments (e.g., the German company Rheinmetall has offered to build a factory in Ukraine to produce Lynx KF41 infantry fighting vehicles and KF51 Panther main battle tanks). The U.S. and the European Union have pledged to support the rebuilding of Ukraine's armaments industry, although it appears that most of the effort to do so will be postponed until after the war.

1.2.1 Conclusion

There are many similarities between the Ukrainian and Polish defence industries. In both cases, the dominant players are state-owned enterprises. In both cases, unfortunately, permanent underfunding over the past 30 years is bearing its fruit, with the situation in both cases beginning to change about a decade ago. In addition, Polish industry, due to Poland's earlier drive to integrate into the economic, political and military structures of the so-called West (in particular, NATO and the European Union), gained access to Western technologies more quickly. While this meant the takeover of some Polish enterprises - mainly those related to the aerospace industry - by Western corporations, in general, it succeeded in obtaining entirely new opportunities that Ukrainian industry couldn't achieve due to its prolonged stay in Moscow's sphere of influence. In both cases, too, many years of unfavourable phenomena (such as corruption, nepotism, etc.) have reduced the efficiency of armaments production, development and implementation of new types, etc.

In addition, there are apparent common areas where the two sides on a cooperative basis could achieve good results. Among these, the land domain, such as armoured vehicles, anti-aircraft and artillery systems, etc., can be pointed out first and foremost. In some cases, the Polish side has a significant advantage (technologies related to the maritime domain, unmanned systems), in others the Ukraine is more advanced (solutions for the production of transport aircraft). Under such conditions, also due to strategic considerations (community of interests related to curbing Russian imperialism), cooperation seems to be a natural solution.

Panther KF51

Source: Rheinmetall Defence, Wikimedia Commons, CC4

Sources

[1] Polska Grupa Zbrojeniowa is one of the largest defence corporations in Europe; "About us", Polska Grupa Zbrojeniowa, accessed May, 25, 2023, https://grupapgz.pl/en/about-us/.

2

Potential areas of cooperation between Polish and Ukrainian arms companies

Dariusz Materniak

2.1 Polish and Ukrainian military cooperation

The establishment of Polish-Ukrainian relations in the military area - both between the armed forces and the arms industry sector became possible when both countries gained the opportunity to pursue independent foreign and security policies. Such an opportunity arose in the late 1980s and early 1990s, as a result of the changes that led to democratisation in the countries of Central and Eastern Europe and the collapse of the USSR (1991). Polish-Ukrainian relations quickly gained a formal and legal framework on the basis of the following agreements: on good neighbourhood (1992) and military cooperation in 1993. Military cooperation was carried out both bilaterally and multilaterally: initially mainly within the framework of NATO's "Partnership for Peace" program, and later also during peacekeeping and stabilisation operations (including in Kosovo, Iraq and Afghanistan). As a natural consequence of closer contacts and exchange of experience, it quite quickly became a desire to develop cooperation also in the field of arms industry sectors.

Ukrainian Soldiers in Iraq Source: Rodney Foliente, U.S. Army, Wikimedia Commons, CC0

Military-technical cooperation is based on documents signed by the defence ministers of both countries in 1996. Over the next nearly two decades, it was carried out mainly in the framework of contacts and working groups dealing with missile technologies, armoured equipment, modernisation of helicopters, telecommunications technologies, anti-aircraft defence, as well as implementation of NATO standards in terms of military equipment in use. This was important for Poland, as an aspiring country and then already a member of NATO, as well as Ukraine, as a country associated with the Alliance and participating in joint military operations.[2] The cooperation concepts discussed at the time included modernisation of helicopters, aircraft, tanks and other armoured vehicles; this was facilitated by simi-

Maidan Uprising **Source: Mstyslav Chernov, Wikimedia Commons, CC3**

larities arising from the common "pedigree" of most types of armaments. At the time, however, no major cooperation project unfortunately lived to see practical implementation.

2014 and the changes that followed Ukraine's "Revolution of Dignity" at that time caused Ukraine to take an unambiguously pro-Western course in its foreign policy. This was also, or even primarily, translated into the military sector - both the army itself and other power structures, orienting themselves henceforth exclusively towards cooperation with Western countries (which resulted primarily from the annexation of Crimea and Russian aggression in the Donbass). The same trend also applied to the arms industry sector. Ukrainian companies increasingly began to look for opportunities to cooperate with Western entities, so as to meet the needs of the security sector involved in the warfare in the east of the country; Poland was a fairly obvious choice here. The Polish arms sector proved to be a key partner for meeting the basic needs of the Ukrainian army in the early stages of the conflict with Russia in Donbass, including helmets and bulletproof vests: a contract with the Polish company "Lubawa" was concluded by the Ukrainian side in the summer of 2014.[3] "Flyeye" drones, manufactured by "WB Electronics" (they have been used by the Ukrainian Armed Forces since 2015; further deliveries were made in 2022), as well as equipment from several other manufacturers, including PCO, Delta Optical and many others, have also been delivered to Ukraine.[4]

The development of contacts between Polish and Ukrainian arms companies has also resulted in new concepts and proposals for modernising military equipment. At the MSPO arms fair in 2016 and 2017, proposals for modernising the T-72 tank, known as the PT-16 and PT-17 were presented.[5] The latter design

2S1 Gvozdika **Source: Wikimedia Commons, CC0**

was developed by " Bumar-Łabędy" in cooperation with UkrObronoProm, a Ukrainian conglomerate, and included suspension reinforcement, engine replacement, installation of a new 120mm calibre cannon and opto-electronic systems.[6] Also at MSPO 2017, the "Stokrotka" missile system, developed by WB Group and UkrObronoProm was presented, intended to combat, among other things, drones and helicopters.[7] Poland and Ukraine also cooperated in the production of the light armoured vehicle "Dozor-B/Oncilla".[8] However, in view of technical problems, its production has not yet been implemented on a larger scale – the first small batch of these vehicles was accepted for arming the Ukrainian Armed Forces in 2020.[9] Between 2016 and 2022, Polish companies were also intermediaries in the supply of equipment for the Ukrainian Armed Forces, including, among others, BMP-1 infantry fighting vehicles and 2S1 howitzers "Goździk".

2.2 Identification of areas of cooperation between the Polish and Ukrainian arms industries

Two factors are of key importance from the point of view of the development of cooperation between the Polish and Ukrainian arms sectors. The first is the potential of enterprises and research centres located in both countries and the resulting capacity to develop new and improve existing technological solutions. This potential is known to exist and to be able to work for cooperation - this was the case both before and after February 24, 2022. The second important - and unique - factor is the experience gained from the warfare in the time since the beginning of the massive Russian invasion of Ukraine on February 24, 2022.

From unofficial sources, one can hear that at least a few Ukrainian factories have been located on Polish territory, primarily engaged in the repair of damaged military equipment (some of the repair work is most likely to be carried out by Polish companies as well; this applies mostly, but not only, to those types of armaments that were previously manufactured/serviced in Poland). Most likely, some types of armaments are also manufactured in Poland by Ukrainian companies that moved from Ukraine after February 24, 2022 (including unmanned aircraft), but the detailed information on this subject is covered by secrecy.[10]

Polish-Ukrainian cooperation in the arms sector has many prospects. Some of them have been hinted at below. However, due to the limited framework of the text, it is not possible to discuss all of them.

PT 91 Twardy Source: Polish Ministry of National Defence, Wikimedia Commons, CC3

Tanks and infantry fighting vehicles

Poland and Ukraine already have some experience when it comes to working on armoured equipment designs. Both the Ukrainian Armed Forces and the Polish Army still have a very large number of armoured vehicles originating from the Warsaw Pact era - despite the modernisation implemented successively by Poland since the 1990s, as well as the supply of Western-made equipment that began to arrive in Ukraine in 2022. It is worth mentioning at this point that much of the military aid from countries such as Poland, the Czech Republic and Slovakia in the segment of tanks and infantry fighting vehicles are post-Soviet designs: mainly T-72 tanks and BMP-1/2 infantry fighting vehicles of various modifications.

Be that as it may, vehicles of Soviet origin constitute, and will continue to constitute for a long time to come, a significant percentage within the armoured vehicle fleets used by the armed forces of Poland and Ukraine: simultaneous replacement of all vehicles of this type exceeds the financial and production capacity of any country, while the combat value of such equipment remains highly questionable. A partial solution to this

IFV Borsuk Source: Matthew Foster, Wikimedia Commons, CC0

Dozor-B **Source: VoidWanderer, Wikimedia Commons, CC4**

problem is to modernise these vehicles to increase their performance capabilities on the modern battlefield: this is indicated by Polish experience with T-72 tanks upgraded to the PT-91 standard, and later in cooperation with Ukrainian partners (PT-16/17). Also, the experience of the Ukrainian armaments complex regarding the modernisation of post-Soviet T-64/72/80 tanks (as well as the known cases of "rapid" armouring of T-72M/M1R tanks handed over to Ukraine in 2022) indicates that there are great opportunities for cooperation in this area. In the case of tanks, the main beneficiary of such activities is likely to be Ukraine, which has already received some 300 T-72 tanks of various modifications from Poland, and according to the announcement of Polish Defence Minister Mariusz Błaszczak after the Ramstein Group meeting on January 20, 2023, is expected to receive more.[11]

Ukraine also received BMP-1 infantry fighting vehicles, but Poland has a large enough stock of this type of vehicle that it can be assumed that a certain part of it will remain in service in Polish Army units for years to come, until such a number of IFV (infantry fighting vehicle) "Borsuk" is produced that will satisfy the needs of Land Forces units.[12] The BMP-1-type vehicles remaining in service will require modernisation - otherwise their combat value will remain, as has been said, low.

War in the Donbass **Source: Source: Teteria Sonnna, Wikimedia Commons, CC2**

The above applies primarily to outdated weapon systems. Both in Poland as well as in Ukraine,[13] efforts have been made to modernise this type of vehicle: the Ukrainian side has repeatedly presented its proposals in this regard at the "Arms and Security" fair held annually in Kiev (including in 2017 and 2018). These included the BMP-1U " Szkwał" (instead of a standard turret with a 73mm 2A28 "Grom" cannon, a "Szkwał" combat module with a 30mm cannon and "Barier" ppk launchers was mounted), the BMP-1UM/UMD (with, among other things, an enlarged landing compartment and a new German engine), and several other.[14] Implementation of such a modernisation program for the Polish Army would be a solution worthy of consideration.

The Ukrainian side remains interested in the production and development of light armoured vehicles of the "Dozor-B/Oncilla" type.[15] In addition, work on land-based drones may become an interesting direction for cooperation in the long term. Several such designs (technology demonstrators) have been developed by Ukrainian companies in recent years. This is, for example, the RSWK-M "Hunter", a land drone designed by the company "KB Robotics", capable of performing reconnaissance, transport and combat tasks, it also has the ability to mount armament: machine gun, grenade launcher or anti-tank missiles.[16] It should be assumed that the role of such systems on the modern battlefield will steadily grow: analogous solutions are being developed in other countries, and in Russia they have already been adopted for armament (robots "Uran-9").

Artillery

Artillery is crucial to the conduct of combat operations in any armed conflict - the battles that are taking place in Ukraine's war with Russia are confirmation of this regularity.[17] It concerns not only the phase of the massive Russian invasion, but also the fighting that took place in eastern Ukraine during ATO/OOS beginning in April 2014,[18] with a special focus on the clashes in late 2014 and early 2015, during the so-called Battle of Debaltsevo.[19] Poland has delivered at least 54 "Krab" howitzers to Ukraine in 2022, which have received very high marks from Ukrainian artillerymen. The experience they have gathered can be used to further improve this design: both the AHS "Krab" itself and the command vehicles and other elements of the "Regina" fire module, especially since the Ukrainian side has ordered more "Krab", in numbers at least as many as have been delivered so far.[20]

The Ukrainian side is also interested in purchasing self-propelled mortars of the "Rak" type with a calibre of 120mm. As agreed and signed during a visit to Poland by Ukrainian President Volodymyr Zelensky (April 5, 2023), so far the Ukrainian Armed Forces are to receive three company fire modules, a total of 24 units of "Rak". While in Poland they are placed on the chassis of the "Rosomak" wheeled armoured personnel carrier, the possibility of placing the turret of the Polish "Rak" on the chassis of the Ukrainian-produced BTR-4 armoured personnel carrier is being considered for procurement for Ukraine in the long term.[21] In the long run, both the one and the other mentioned construction may turn out to be an export product.
There is also room for cooperation when it comes to the production of ammunition: first of all, "ordinary" artillery ammunition of "NATO" calibre, i.e. 155mm, but also "Soviet" 152mm, which is still used by the Ukrainian Armed Forces. The above-mentioned area of potential cooperation also extends to precision artillery ammunition: the Ukrainian side has developed a projectile of this type under the name "Kvitnyk", which can be produced in versions for both the above-mentioned calibres. Missiles with analogous characteristics "Karasuk" and "Krucha" of 122mm - artillery calibre and 120mm - mortar calibre are also being designed.[22] Also in Poland there was work on artillery shells of 120mm and 155mm calibre,[23] which, in perspective, provides

Sokil-300

Source: VoidWanderer, Wikimedia Commons, CC4 opportunities for joint work and improvement of this type of ammunition.

Reconnaissance and strike drones

While the use of drones is nothing new - either in the armed conflicts of the past few decades, or even more so in the case of the military operations taking place on Ukrainian territory since 2014, the current war has brought the most massive use of drones of any kind in the history of armed conflict to date.[24] Ukraine uses many types of drones: from specialised designs such as the BSL "Furia" produced by the Kiev-based "Atlon Avia" company (designed for reconnaissance tasks and correcting artillery fire), the Turkish "Bayraktar", the Polish reconnaissance "Flyeye" and strike "Warmate" to commercial drones of various types, adapted for strike and/or reconnaissance tasks.

Reconnaissance activities are the vast majority of tasks performed by drones during combat on Ukrainian territory: this includes missions carried out in support of artillery or mechanised units, but also special forces combat teams (which often use their own drones capable of being transported by such a team, such as the US RQ-11 "Raven"). This situation provides ample opportunities to gain experience on the use of drones in various conditions and situations, for the performance of many types of tasks, and thus offers opportunities for the extensive development of new and improved designs, more resistant to interference, radio combat systems or other means of combat (this also applies to anti-drone systems and all aspects of their use). At the beginning of 2023, separate infantry companies equipped with drones (reconnaissance and strike drones), as well as communications and other equipment were created in the Ukrainian Armed Forces on the basis of past experience under the "Drone Army" project. Their task is to carry out strike operations in vital areas of the front line. A staff cell established within the framework of the aforementioned project is to analyse the conclusions of ongoing operations and implement appropriate adjustments related to the use of this type of weaponry.[25]

According to the available data and opinions, the Polish unmanned drones "Flyeye" and "Warmate" have performed very well in operations in Ukraine, demonstrating good technical parameters, as well as resistance to the enemy's EW (Electronic Warfare) means. This experience will certainly be used in the development of the next design, i.e. the "Gladius" search and strike system. The contract for the delivery of the first four modules of this type by WB Group was signed in May 2022. This system consists of two types of drones: the FT-5 reconnaissance drone and the BSP-U strike drone, operating through coordination through the Integrated Battlefield Management System "Topaz".[26] In September 2022, a contract was signed for the development of the "Gladius-2" system.[27] It can be assumed that they will widely take into account the experience of using elements of already existing systems by the Ukrainian Armed Forces in the war with Russia.

US RQ-11 Raven **Source: Alejandro Peña U.S. Air Force, Wikimedia Commons, CC0**

Ukraine also has experience when it comes to the use of Bayraktar-type drones in combat conditions. Several dozen UAVs of this type were already on the equipment of the Ukrainian Armed Forces at the outbreak of the war, and more were delivered after February 24, 2022. "Bayraktar" is also expected to be included in the inventory of the Polish army. Lessons related to their operation in combat conditions will be relevant for Poland as well. The Ukrainian arms sector has also developed a project for its own unmanned aircraft of a similar class (reconnaissance and strike) called "Sokil-300" - the concept was presented in late 2020. In the long term, the potential of the two countries to design and build drones could result in further, more advanced designs. This makes sense insofar as the importance of UAVs on the modern battlefield will grow.

Gepard

Source: Hans-Hermann Bühling, Wikimedia Commons, CC3

Defence against drones is also a challenge for the Ukrainian army and defence companies, but also for any future battlefield. This applies to both reconnaissance and strike systems. In the case in question, losses on the Ukrainian side in the course of fighting in 2022 and early 2023 were inflicted by Russian "Lancet" type drones, also in the case of the AHS "Krab" used by the Ukrainian Armed Forces.[28] The task for the Polish and Ukrainian arms sectors will be to develop effective capabilities to combat this type and similar UAVs.[29] So far, available means are being used for this purpose, so among others, anti-aircraft kits such as the "Gepard" or ZSU-23, but ultimately it is necessary to develop additional solutions to ensure greater effectiveness: especially since over time there will probably be more drones of newer types, with greater potential effectiveness of operation.[30]

Carbines, grenade launchers and anti-tank missiles

Poland has supplied Ukraine with about 10,000 "Grot" type carbines and there are many indications that the deliveries will not end there, especially since the conflict is likely to continue, and this will require further deliveries of armaments, including light weapons.[31] The number of "Grot" carbines will also increase in the Polish army - in early January 2023 a contract was signed for the delivery of another 70,000 weapons of this type. There is yet no official data in the public space (from the Ukrainian or Polish manufacturer's side) on how this weapon performs, although based on user testimonies and analyses appearing in the Ukrainian media, one can conclude that it is a weapon well adapted to the conditions of the current conflict. Probably, information on the operation of this weapon, including data on possible failures, opinions of soldiers, etc., will be important for the manufacturer - the Weapons Factory in Radom, for which (quite significant) deliveries to Ukraine are a chance to check the properties of the "Grot" carbine (in the A1 version after minor modifications) in real combat conditions. In the long run, theoretically - if the findings from use continue to be positive - a carbine of this type could become the basic automatic carbine of the Ukrainian army. The question of the possible place and form of production and supply (production in Poland, purchase of a license) is a matter of further arrangements between the Polish and Ukrainian sides.

If we are talking about cooperation in the development of light weapons systems, then in addition to the "Grot" carbines, other constructions should be considered: anti-tank missiles and grenade launchers. Ukraine has extensive anti-tank capabilities, based both on its own designs (e.g. "Stugna-P", "Korsar") and on foreign supplies (e.g. "Javelin", "NLAW"). Poland and Ukraine have jointly developed the "Pirat" anti-tank missile - the result of cooperation between the "KB Łucz" enterprise from Ukraine and the Polish "Mesko S.A.", using, among other things, Ukrainian experience with the "Korsar" missile, as well as Polish elements of the guidance and control system. It is intended that this missile will complement the anti-tank capabilities in the Polish army, in parallel with the "Javelin" missiles, and alongside the "Spike" and anti-tank grenade launchers.[32]

Another design to be equipped by the Ukrainian army in 2022 is the RGP-40 revolver grenade launcher, manufactured by "ZM Tarnów". Also in this case, the experience of using the grenade launcher in real battlefield conditions will guide the manufacturer when it comes to implementing improvements and possible modifications, as in the case of other designs that have not previously been used in the realities of a similar armed conflict, that have only been used to a limited extent.

Space technology

Space is an environment that is becoming increasingly important in the conduct of military operations, espe-

Grim 2 tactical missile

Source: VoidWanderer, Wikimedia Commons, CC4

cially in terms of satellite reconnaissance and communications capabilities. Ukraine has certain capabilities when it comes to the ability to produce missiles and launchers, allowing satellites to be launched into orbit: these are primarily the capabilities of the "Yuzhmash/Pivdenmash" plant in Dnipro. Among other things, these plants produce "Zenit" rockets, mainly for the Sea Launch consortium.

The coordination of space industry activities is handled by the State Space Agency of Ukraine. Although the activities of the above-mentioned facilities were severely curtailed after 2014 in connection with the severance of cooperation with Russia, it has broad prospects: also in terms of the possibility of establishing cooperation with the Polish Space Agency in the implementation of both military and scientific-research projects. It is worth remembering that the role of space as an environment relevant to the conduct of military operations will steadily grow: in the medium-term perspective mainly when it comes to reconnaissance, in the long-term also when it comes to typically kinetic systems.

In addition, Ukraine is interested in cooperation with Poland when it comes to further development of missiles, including short-range ballistic missiles (a project opera-

Neptune cruise missile

Source: President of Ukraine, Wikimedia Commons, CC4 ting under the names Sapsan/Grom-2), especially when it comes to work on rocket fuel. It should be expected that the development of this design will be possible after the end of the active phase of military operations.[33]

Navy

In the case of both Poland and Ukraine, a lot of investment is required by naval forces. In the case of the Polish Navy, this is due to years of reduced spending on this type of armed forces; in the case of Ukraine, it is primarily the result of the loss of most of its ships and much of its facilities following the annexation of Crimea in 2014. Ukraine's Naval Forces have acquired a number of ships from the US; further deliveries were to be made by the UK (minesweepers and missile boats) and Turkey (a contract for the purchase of corvettes; one is under construction), but these plans were hampered by the start of the Russian invasion on February 24, 2022.

Even if the indicated ship acquisition plans live to see implementation, the Ukrainian Navy will need more vessels with greater combat capabilities to secure the country's interests in the Black Sea - and we are talking about a time perspective of several years or more. It may be advisable to consider cooperation with Poland in the construction of warships: both mine destroyers of the "Kormoran II" class (three units of this type have already been built for the MW of the Republic of Poland; the construction of three more is planned), but also missile frigates to be built under the "Miecznik" program. Significantly, the co-operator of the PGZ-Miecznik consortium will be companies from the British arms sector, which should further stimulate cooperation between Poland, Ukraine and the UK in this field.[34] Another interesting area is the potential for cooperation in the production and operation of underwater and surface drones, especially given the Ukrainian experience with the use of the latter against ships of the Russian Black Sea Fleet,[35] as well as those concerning the use and possible joint production of "Neptune" anti-ship missiles or their development versions.

Lithuanian–Polish–Ukrainian Brigade Symbol Source: Wikimedia Commons, CC4

2.3 Barriers and major challenges

From the point of view of the desirability of cooperation between companies of the arms complex, the key is the demand for a given equipment or technological solution from representatives of the armed forces and other formations of the state security sector. One of the most important elements allowing to obtain such experience and, on the basis of it, to develop appropriate conclusions (and further implementation) are structures allowing to develop contacts and cooperation between armies. In the case of Poland and Ukraine (and Lithuania), one such element is the LITPOLUKRBRIG Multinational Brigade, the command of which has been located in Lublin since 2015. Training cooperation was also carried out within the framework of the NATO JMTG-Ukraine (Joint Multinational Training Group - Ukraine) mission established for this purpose, operating until early 2022 at the training centre of the Ukrainian Armed Forces in Yavoriv (Lviv region). Contacts are also carried out on the occasion of joint exercises and manoeuvres, but also within the framework of military attaché, as well as contacts of expert, scientific and similar circles - also within the framework of conferences or fairs.

While many concepts and ideas for cooperation or technological solutions, modernisation and changes, as well as designs for new weapons systems may be pertinent and potentially useful for the armed forces of the cooperating countries, there are barriers to such cooperation. It is no different in the case of Poland and Ukraine: despite the commonality of strategic goals and the constantly improving communication between the two countries, there are still - and especially in the current circumstances - limitations that will hinder the development of cooperation, including in the arms sector.

The most serious problems for the development of cooperation primarily include those indicated below.

War

While the ongoing conflict is a factor conducive to the development of weapons systems and their improvement on the basis of battlefield experience, at the

Hospital in Mariupol after Russian airstrike **Source: ArmyInform, Wikimedia Commons, CC4**

same time, of course, it negatively affects the ability of both industry and the scientific and research sector to function and international cooperation - if we are talking about a country that is a party, in the case under discussion - a country defending itself against aggression by a stronger opponent.

In the case at hand, this is primarily due to the damage caused by missile and air strikes targeting the centres of Ukraine's arms industry. These attacks caused some damage to industrial infrastructure, including the armaments sector. In view of the timely decision to evacuate/relocate some of the plants and their equipment from known locations to sites provided for these purposes in time of war, the irreparable losses are less than they would have been without taking such steps. Nonetheless, many of them have and will continue to affect the health and viability of companies in this industry. Additional difficulties in wartime include restrictions on the supply of energy resources (especially electricity - in view of attacks on energy infrastructure), the prioritisation of company activities aimed at overhauling and quickly restoring operational readiness of military equipment, as well as the temporary (called up for military service, wounded, injured) and permanent (killed, permanently maimed) attrition of engineering and other groups of personnel necessary to carry out the work of armaments companies. Coping with these problems will take time probably counted in years.

Vasyl Lozinskiy Ukraine's deputy infrastructure minister

Source: Lviv Regional State Administration, Wikimedia Commons,CC4

Euromaidan Source: Ilya, Wikimedia Commons, CC3

Corruption

The issue of corruption remains a serious problem for Ukraine. Since the "Revolution of Dignity" and the changes that took place as a result, the Ukrainian state has made significant progress in terms of implementing mechanisms and principles to combat corruption. Changes have been made to the law, the judiciary, and appropriate institutions have been established that specialise in fighting this phenomenon, including NABU - the National Anti-Corruption Bureau of Ukraine. And, what is particularly important, the social acceptance of corrupt practices and actions has fundamentally decreased. After 2014, a civil society finally emerged in Ukraine, with an awareness of its capabilities and the ability to influence the actions of state authorities. Importantly, the newly established institutions are open to cooperation with Western countries when it comes to combating corruption - this includes Polish-Ukrainian cooperation in this area.[36] This, moreover, is the requirement of countries such as the US or financial institutions (e.g. the IMF or the World Bank) - as financial and economic assistance is conditional on the implementation of changes in the fight against corruption.

Despite this, it would be naïve to think that the problem in question has been eliminated entirely within the few years since the last Ukrainian revolution. How deep the issue is can be seen by the detention of one of the deputy ministers, Vasyl Lozinskiy, on charges of accepting a bribe in connection with generator purchases in recent months, when the massive shelling of Ukraine's energy infrastructure began.[37] Detentions, though on other charges most likely not without financial threads also do not bypass companies in the arms sector, such as "Motor-Sicz".[38] All this means that the establishment and development of business cooperation, including in the arms sector, will face problems related to such phenomena.

Bureaucracy

Formal issues are a significant problem in contacts between business representatives from different countries, even more so operating in different formal, legal and organisational realities. This is the case of Poland, which has been a member of the European Union for nearly two decades - and Ukraine, which so far remains outside the EU. The signing and implementation of the EU-Ukraine Association Agreement (2014) had a positive impact on reducing these barriers, but did not remove them completely. It will take many more years to change the legal and organisational culture in this area, even assuming that the process of Ukraine's integration into the EU is accelerated, as it was with candidate status.

A facilitating factor in overcoming such difficulties is the mental and cultural proximity of Poles and Ukrainians. Many issues that are difficult from a formal point of view are definitely easier to "get along" first on informal grounds, and only later to look for an appropriate legal and organisational framework.[39] Companies intending to implement or already implementing Polish-Ukrainian cooperation projects, including in the arms sector, should receive appropriate support from diplomatic and consular services. A common, clear vision of further cooperation is also needed, with an indication of specific projects and programs in which cooperation can bring tangible benefits to both sides.

2.4 Summary

Cooperation between Poland and Ukraine on joint projects in the arms industry sector has broad prospects. A number of factors work in its favour: first and foremost, the high convergence of the two countries' strategic interests in the area related to security and defence in the broadest sense, a similar perception of security threats and challenges, the mental and cultural proximity of the two nations, as well as the already existing experience of cooperation, both at the level of the armed forces of the two countries and enterprises in the armaments sector. While Ukraine is at war and gains a range of experience in the use of military equipment on the battlefield from this, Poland plays, among other things, the role of a logistics base, extremely important in the sphere of current supplies, but also for repairs as well as for the production of necessary means of warfare. Over time, this role will become increasingly important for Poland.[40] The synergy of Ukrainian experience and Polish technological capabilities is likely to bring tangible benefits. A prerequisite for this, however, is taking advantage of emerging opportunities, as well as dealing with the challenges posed by current conditions.

Sources

[1] A. Sławiński, „Główne kierunku polsko-ukraińskiej współpracy wojskowej po 1991 roku", De Securitate et Defensione, issue 8 nr 2 (2022), https://desecuritate.uph.edu.pl/images/9._Slawinski_De_Securitate_no._1_2020.pdf.

[2] Ibidem.

[3]„Hełmy i kamizelki dla ukraińskiego MSW", Lubawa SA, accessed January 25, 2023, https://lubawa.com.pl/pl/2014/1917-helmy-i-kamizelki-dla-ukrainskiego-msw.

[4] A. Świerkowski, „Więcej polskich bezzałogowców na Ukrainie". Defence24, accessed January 27, 2023, https://defence24.pl/sily-zbrojne/wiecej-polskich-bezzalogowcow-na-ukrainie.

[5] A. Kiński, „PT-16 – kolejne ogniwo w ewolucji Twardego", ZBiAM, accessed January 23, 2023, https://zbiam.pl/artykuly/pt-16-kolejne-ogniwo-w-ewolucji-twardego/.

[6] K. Wasilewski, „PT-17, czyli modernizacja Twardych", Polska Zbrojna, accessed January 23, 2023, https://www.polska-zbrojna.pl/home/articleshow/23549?t=PT-17-czyli-modernizacja-Twardych.

[7] J. Sabak, „MSPO 2017: Polsko-ukraiński system rakietowy „Stokrotka", Defence24, accessed January 26, 2023, https://defence24.pl/sily-zbrojne/mspo-2017-polsko-ukrainski-system-rakietowy-stokrotka.

[8] The names are often used interchangeably, while the manufacturer, Mista Ltd. emphasizes that the two designs are different; O. Katkov, „Oncilla ma być ukraińskim pojazdem", Defence Express, nr 5-6 (2021), p. 36-38. R. Muczyński, „Mista dostarcza po R. [9] Muczyński, „Mista dostarcza pojazdy Oncilla na Ukrainę", MilMag, accessed January 23, 2023, https://milmag.pl/mista-dostarcza-pojazdy-oncilla-na-ukraine/.

[10] Based on talks with representatives of the Ukrainian arms sector.

[11]„Польща передасть Україні танки Т-72 та БМП, accessed January 25, 2023, https://mil.in.ua/uk/news/polshha-peredast-ukrayini-tanky-t-72-ta- bmp/?fbclid=IwAR3KKZv3ggTqqUyCuVbg1QSn-3ZB4Anpr35sP1HXysEUgyedcj0rL7ZCkLwU.

[12] Production capacity is estimated at about 1,000 vehicles over 10 years; M. Szopa, „Ile Borsuków dla wojska? PGZ przedstawia liczby", Defence24, accessed January 22, 2023, https://defence24.pl/przemysl/ile-rocznie-borsukow-z-pgz.

[13] In Poland in the 1990s, among other things, a BWP-2000 was developed with an OTO Melara turret and a 60mm automatic cannon. In the end, only two prototypes were built; „BWP-2000: Prototype infantry fighting vehicle", Military Today, accessed January 23, 2023, http://www.military-today.com/apc/bwp_2000.htm.

[14] J. Sabak, „Ukraina: Cztery wieże do modernizacji BMP-1[ANALIZA]", Defence24, accessed January 23, 2023, https://defence24.pl/przemysl/ukraina-cztery-wieze-do-modernizacji-bmp-1analiza.

[15] Based on talks with representatives of the Ukrainian arms sector.

[16] O. Katkov, „Narodzone na polu walki", Defence Express, nr 3-4 (2021), p. 24-27.

[17] „Artyleria potwierdza skuteczność na Ukrainie. Jakie wnioski dla Polski? [INTERVIEW]", Defence 24, accessed January 20, 2023, https://defence24.pl/sily-zbrojne/artyleria-potwierdza-skutecznosc-na-ukrainie-jakie-wnioski-dla-polski-wywiad.

[18] ATO - Anti-Terrorist Operation (Ukr. Anti-Terrorist Operation), OOS - Operation of the Combined Forces (Ukr. Operation of the Overtaken Forces).

[19] More on this: Ł. Nadolski, Kampania zimowa 2015 roku na Ukrainie, (Bydgoszcz: Muzeum Wojsk Lądowych, 2017).

[20] M. Szopa, „Polska sprzedała Kraby Ukrainie. Rekordowy kontrakt", Defence24, accessed January 22, 2023, https://defence24.pl/przemysl/polska-sprzedala-kraby-ukrainie-rekordowy-kontrakt.

[21] Based on talks with representatives of the Ukrainian arms sector.

[22] S. Zgurets, "Straight on target", Defence Express, accessed Janaury 23, 2023, https://en.defence-ua.com/industries/straight_on_target-1647.html.

[23] P. Gurgurewicz, „Przeciwpancerny Pirat z Mesko", MilMag, accessed January 26, 2023, https://milmag.pl/przeciwpancerny-pirat/.

[24] Another conflict where drones also played a significant role was the fighting for Nagorno-Karabakh in 2020, although in that case the scale - both of the use of UAVs and the conflict itself - was significantly smaller.

[25] Т. Лозовенко, „У ЗСУ формують перші у світі ударні роти безпілотників – Генштаб", Ukrainska Pravda, accessed January 28, 2023, https://www.pravda.com.ua/news/2023/01/27/7386822/.

[26] Ministry of Defence, „Bezzałogowce Gladius", Ministry of National Defence Republic of Poland, accessed January 23, 2023, https://www.gov.pl/web/obrona-narodowa/drony-gladius.

[27] „Praca rozwojowa na drony uderzeniowe nowej generacji GLADIUS-2", DlaPilota, accessed January 23, 2023, https://dlapilota.pl/wiadomosci/polska/praca-rozwojowa-na-drony-uderzeniowe-nowej-generacji-gladius-2.

[28] Ukraine has developed, similar to the „Lancet" ST-35, „Grom" strike drones; flight tests took place in 2020 and 2021; O. Katkov, „Narodzone na polu walki", Defence Express, nr 3-4 (2021), p. 24-27.

[29] Poland already has some capabilities in this area and they are being used by Ukraine, among others, to combat Iranian kamikaze drones; M. Dura, „Polish Jastrząb' tracks Iranian kamikaze drones", Defence24, accessed January 29, 2023, https://defence24.pl/polski-jastrzab-tropi-iranskie-drony-kamikaze.

[30] J. Sabak, „Rosyjska amunicja krążąca Lancet-3. Pogromca ukraińskiej artylerii czy gwiazda rosyjskiej propagandy? [ANALYSIS]", Defence24, accessed January 24, 2023, https://defence24.pl/wojna-na-ukrainie-raport-specjalny-defence24/rosyjska-amunicja-krazaca-lancet-3-pogromca-ukrainskiej-artylerii-czy-gwiazda-rosyjskiej-propagandy-analiza.

[31] Z. Lentowicz, „Jeszcze więcej karabinków Grot dla armii", Radar, accessed January 20, 2023, https://radar.rp.pl/przemysl-obronny/art37715671-jeszcze-wiecej-karabinkow-grot-dla-armii.

[32] A. Kiński, „Pirat - szansa na realne wzmocnienie polskiej obrony przeciwpancernej", Wojsko i Technika 6 (2020).

[33] Based on talks with representatives of the Ukrainian arms sector.

[34] K. Wilewski, „Miecznik. Nowy wymiar marynarki wojennej", Polska Zbrojna, accessed January 24, 2023, https://www.polska-zbrojna.pl/home/articleshow/37204?t=Miecznik-Nowy-wymiar-marynarki-wojennej.

[35] „Ukraina ujawniła szczegóły dotyczące nawodnych systemów bezzałogowych", Militarnyi, accessed January 20, 2023, https://mil.in.ua/pl/news/ukraina-ujawnila-szczegoly-dotyczace-nawodnych-systemow-bezzalogowych/.

[36] „Ukraińskie NABU będzie współpracować z CBA", Wydział Informacji i Edukacji Antykorupcyjnej GSz CBA, accessed: January 22, 2023, https://antykorupcja.gov.pl/ak/aktualnosci/12115,Ukrainskie-NABU-bedzie-wspolpracowac-z-CBA.html.

[37] Р. Петренко, „Затримання заступника міністра: НАБУ розповіло деталі схеми з генераторами", Ukrainska Pravda, accessed January 25, 2023, https://www.pravda.com.ua/news/2023/01/22/7385976/.

[38] P. Auguff, „Ukraińskie media ujawniają. Podejrzany o współpracę z Rosją szef firmy Motor Sicz", Dziennik, accessed January 24, 2023, https://wiadomosci.dziennik.pl/swiat/artykuly/8574371,ukraina-rosja-wojna-motor-sicz-bohuslajew-rosyjskie-obywatelstwo-paszport.html.

[39] The above statement is supported by the author's personal experience of several years in the framework of ongoing Polish-Ukrainian projects.

[40] „Head of British defense commission: a large arms factory for Ukraine should be built in Poland.", Business Insider, accessed January 30, 2023, https://businessinsider.com.pl/gospodarka/szef-brytyjskiej-komisji-obrony-w-polsce-powinna-powstac-wielka-fabryka-broni-dla/2qdcbzq.

3

Potential financing sources for Polish-Ukrainian military projects

Paulina Zamelek, Ph.D

3.1 Brief overview

European Union has got at its disposal several tools that could possibly support the financing of the Polish-Ukrainian military projects. Speaking about the European Union (EU) sources only, it's necessary to start the analysis with the Horizon programmes, and the projects under the EDA and PESCO umbrella. However, a support for scientific and research projects could be also considered through other sources, including NATO.

3.2 European steps towards defence projects financing

Looking at the reforms undertaken in the frames of the Common Security and Defence Policy,[1] one can notice a great emphasis placed on research and development activities. Security, defence and space issues as well as dual-use innovations are getting high on the EU agenda in the last decade and tend to serve a priority for financing in the next decades, which reflects the development in the geopolitical, military, technological and globalisation fields. The growing overlap between civilian and military operations is evident as a trend, which increases the EU interest in all aspects related to defence, space and security.

Source: European Defence Agency, CC0

Early steps in financing EU research projects in the security field can be traced back from 2003 with an initiative to develop a European security research programme (ESRP), which eventually in the years 2004-2006 supported 39 projects in up to 65 mil € (mostly in areas of access and border control, ICT and surveillance systems). The next step was 7th Framework Programme for Research (FP7, 2007-2013) for exclusively civil orientation. However, budget of 1.4 bn € was devoted to ESRP cooperation programmes for thematic areas close to space, security and dual use potential.

The EU financing then continued in the 8th Framework Programme for research and innovation (Horizon 2020, 2014-2020) already with a magnitude of security, space and defence related projects. The striking thing about the security and defence research and development (R&D) projects in Horizon 2020 (and earlier as well), as the analysis shows, is that almost half of them were related to cybersecurity. And still about 90% of all the EU co-financed projects in that timeframe had potential dual-use application with the output to be used both in civil and defence sectors.[2]

Eventually, the EU initiated a fully-fledged defence research programmes under the Horizon Europe framework (2021-2027), in particular in the frames of the European Defence Fund). However, a parallel, dedicated track for defence projects have been in progress for years now, thanks to collaboratively financed programmes undertaken by the EU Member States through the European Defence Agency (EDA).

EDA

In 2004, the European Council created an intergovernmental agency to act in the field of developing defence capabilities, research, acquisitions and armaments. In pursuing its mission to develop capabilities in support of the Common Security and Defence Policy (CSDP), the EDA carries out research and technology (R&T) activities. More than a billion Euro has been allocated to about 250 R&T projects since the EDA's creation, both of A category (with all EDA Members participation) and B category (with interested Members participation and financing only). However, the EDA's research activities have not been funded from the EU budget, but came from the participant countries.

R&T activities are managed through the EDA capability technology groups (CapTechs), which form a network of experts from participating Member States (governmental, military, academia, industry sides) dedicated to a particular technology area, and provide strategic guidance on the R&T priorities. There are currently 15 CapTechs, 6 within military capabilities (communication and information systems; systems of systems, battlelab, and modelling & simulation; aerial systems; ground systems; naval systems; and missiles and munitions technologies) and 9 on cross-cutting enablers (materials and structures; technologies for components and modules; radiofrequency sensor technologies; electro-optical sensor technologies; CBRN and human factors; energy & environment; guidance, navigation and control; cyber R&T, and ad hoc working group space defence).[3]

This R&T technology bottom-up push-process at the EDA is systematically strengthened at strategic level from a top-down capability-pull process with a dedicated Overarching Strategic Research Agenda (OSRA), as well as Key Strategic Activities (KSA). The newest consolidating initiative for the EU wide scope concerns additional 2 bn € for EU Defence Innovation Scheme and the Hub for innovation of the European Defence Agency (HEDI).[4]

German military vehicles column **Source: Torsten Meynle, European Defence Agency, CC0**

EDAP

The first EU action solely devoted to defence was the European Defence Action Plan (EDAP). It was announced by the European Commission in 2016 with the aim to support the development of a competitive and innovative industrial base in the defence sector, as well as to develop cooperation and increase the effectiveness of EU Member States' spending on joint defence capabilities.[5] EDAP was the springboard to trigger supporting investments, eventually foreseen in the creation of the European Defence Fund, developing the defence supply chain pillar, as well as a single market for defence.

PESCO

In 2017, the Permanent Structured Cooperation (PESCO) was decided upon by the European Council as the practical example of defence cooperation mechanism to address Union's capability and operational needs. Therefore, PESCO initiatives are not R&D projects per se, but they are closely related to R&D goals and favourable EDF funding. Nevertheless, the participation in PESCO required from Member States also other commitments including: increasing defence budgets, spending on investments (reaching 20%), increasing funds for research and technology (up to 2%), compliance checks and the provision of adequate capacities to achieve a certain level of EU ambition. For that reason PESCO projects may benefit from increased EU co-financing for an extra 10% up to a total of 50%. Now, 5 years later, measurable results of PESCO include 60 projects developed with legally binding nature of commitments undertaken by 25 Member States. The projects address areas such as training, land, maritime, air, cyber, and joint enablers.[6]

For the time being, Poland has declared participation in the following 13 projects: European Medical Command, European Secure Software defined Radio (ESSOR), Network of logistic Hubs in Europe and support to Operations (NetLogHubs), Military Mobility, Maritime (semi) Autonomous Systems for Mine Countermeasures (MAS MCM), Harbour & Maritime Surveillance and Protection (HARMSPRO), Cyber Rapid Response Teams and Mutual Assistance in Cyber Security, Integrated Unmanned Ground System (UGS), EU Radio Navigation Solution (EURAS), Integrated European Joint Training and Simulation Centre (EUROSIM), Special Operations Forces Medical Training Centre (SMTC), EU Collaborative Warfare Capabilities (ECoWAR), and Defence of Space Assets (DOSA).

While membership of the PESCO is restricted only for those Member States who have undertaken the more

Lockheed C-130 Hercules

Source: European Defence Agency, CC0

binding commitments, third States (i.e. Ukraine) may exceptionally be invited to participate in a specific project (as a member or observer) upon meeting certain conditions (meaning political, substantial and legal requirements) set in Article 46(6) of the Treaty of the European Union, like in the previous examples of US, Canada or Norway participation in Military Mobility project. It's also justified by the EU's PESCO requirement to be coherent with NATO members. Two other initiatives, i.e. CADR and EDF are complementary to PESCO in the area of planning and financing.

CADR

Coordinated Annual Review on Defence (CADR) is run by the EDA with the aim to help monitor national defence spending plans to identify opportunities for new collaborative initiatives. Therefore, this initiative by a gradual synchronisation of national defence planning cycles and capability development practices supports the EU Member States' efforts to better identify opportunities for new projects (in particular PESCO projects). Each CADR cycle recommends collaborative opportunity (currently 127) and project proposals (i.e. cyber operations, C-IED and EOD, and medical capabilities) with high-end capability prioritisation.[7]

EDF

European Defence Fund (EDF) was established in the EU in 2021 with the aim to finance the research and developmental works in area of military materiel and defence technologies. It's total budget within the Multiannual Financial Framework for the years 2021-2027 amounts to 7.95 bn €, including 2.65 bn € for scientific research and 5.30 bn € for developmental works.[8] The EDF had its two predecessors to test the EU financing tracks devoted for the first time in Union's history for the projects in defence area. Those pilot cases took place in three tranches: in 2016-2017 with Pilot Project amounting to 1.4 mil €, in 2017-2019 with Preparatory Action on Defence Research (PADR), and in 2019-2020 with European Defence Industrial Development Programme (EDIDP).

PADR was entrusted by the European Commission (EC) to the EDA with the objective to demonstrate the added value of the EU-funded research in the defence sector. This pilot project amounted already to 90 mil €, and funded 18 defence research projects mainly on grant-based scheme, of which the intellectual property rights (IPRs) were owned by the beneficiaries. Areas of interest in PADR were allocated to: electromagnetic spectrum dominance; future disruptive defence technologies; emerging game changers; unmanned systems and platforms; electronic design technologies for defence applications; effects; strategic technology foresight; and force protection and soldier systems.[9]

EDIDP, the new development pilot program launched in the subsequent timeframe targeted defence capability development and was equipped with 500 mil € budget to finance up to 100% of total eligible costs of awarded projects in case of research activities, or 20-80% in case of development projects (from prototyping to certification). The fund did not cover the acquisition costs, although, in order to ensure that the EU resources are put to good use, development of common prototypes

EuroMALE ILA

Source: DeffiSK, Wikimedia Commons, CC4

is funded only when member states intend to buy the final product or use the technology in a coordinated manner. EDIDP resulted in 16 collaborative projects funded in 2019, and subsequent 26 projects in 2020 as a results of the 12 calls for proposals. It's interesting to see in this process the involvement of 420 entities (35% representing SMEs) in 2020 only, with wide geographical coverage including all current, at that point, 26 EU member states' representatives – on average 16 entities located in 7 Member States. Moreover, 10 entities controlled by third-countries or third-countries' entities involved in proposals applied for funding (India, Israel, Japan, Oman, Switzerland and United States). On top of that, in the selection process higher priority was given for the projects established under the PESCO framework – European Medium-altitude Long Endurance Remotely Piloted Aircraft system (MALE RPAS) and European Secure Software defined Radio (ESSOR) as strategic enablers for European defence.[10]

Based on the above cases, the EDF was designed with aim to strengthen competitiveness, effectiveness and innovativeness of the European Defence Industrial Sector, and – above all – to incentivise and support cross-border defence R&D. Thus, the technological and strategic autonomy would increase and facilitate industrial innovation, research and supply chains interoperability for new European defence systems. The fund is designed not to replace Member States' defence investments, but to enable and accelerate their cooperation.

Looking into the details of the EDF, two parts can be distinguished: the research part (window) and the development part. The research projects are in total financed by the EU and do not require the support of participating Member States, although such support could be beneficial if it justified running particular project as a national research priority.[11] Research window for collaborative R&T projects is addressed to consortiums, which need to be established in a response to a particular call for proposals opened by a European Commission. The winning proposal in a competition is the basis to sign a grant agreement between the EC and the consortium partners. Priority areas in this category usually include critical and innovative technologies such as electronics, metamaterials, encryption software and robotics or future disruptive defence technologies.

The second strand, the EDF development (and acquisition) projects (called "capability window") – in line with the wording of the EDF Regulation art. 21 – can be initiated by at least two states declaring that they will procure the final product or use the technology in a coordinated way. This governmental declaration is provided to the EC at the initial stage of submitting a project together with – the so called – Initial Common Requirements, which shall be agreed by the supporting states to provide the basis for technical specifications of what is expected to be achieved in the development project. If the development project wins the competition, then the Memorandum of Understanding (MoU) is signed between the supporting states with detailed engagements.[12]

Ministry of National Defence of the Republic of Poland **Source: Gnesener1900, Wikimedia**

Although the financing scope from the EU budget dedicated to the development projects can range from 20% to 100%, most of the developmental projects actually require national co-financing. Two forms of co-financing are common: a form of industrial contribution from the consortium members' own funds (i.e. demonstrating the costs of using own research infrastructure) and public sources.

The Polish Ministry of National Defence (MoD) financial support for the EDF development projects is considered on case-by-case basis in view of the Armed Forces prospective needs and strengthening the national defence industrial and technological base. For that reason, the MoD recognises two forms of development projects: for equipment and for technologies. Equipment development projects are directed at particular military operational requirement and military materiel procurement needs. However such category of projects did not appear at all in the last two years (2021-22). In contrast, technological development projects are bounded with the military materiel systems (and subsystems) development, as well as technologies of high levels of technological readiness. Majority of the of applied development projects lie in this EDF category since their "topics" are not limited to military operational requirements, but are assessed in view of perspective needs foreseen in current strategic documents.[13]

In May 2022 the EC published the Multiannual Perspective (MAP), which is indicative and supports the EDF multiannual planning process.[14] The MAP is enlisting categories of planned actions in perspective of 2021-2027. However, they do not preclude other tasks or areas to be included in the coming years in the annual work programmes, because these will be defined every year by the European Commission with the participation of the ministries of defence and the EDA, and based on the Action Plan on Synergies between civil, defence and space industries.

The latest call for proposals was launched by the EC in May 2022 together with the EDF Work Program for 2022. Annual work programmes are structured along 17 thematic and horizontal categories of action. Since the beginning of the EDF Program 60 collaborative defence research and development projects have been accepted by the EC (out of 142 proposals) for financing of almost 1.2 billion Euro, including 15 projects coherent with PESCO priorities (the EDF projects list is presented in Table 1.). Analysing the geographical coverage of the already accepted EDF projects, the participation of all EU member states is visible with exceptionally high presence of French (178), Italian (156), Spanish (147), and German (113) entities, but also with a good representation of Greek (75) and Dutch (54) participants. Polish entities are identified in 31 existing projects. The mean number of participants in each project amounts to 18, and those on average represent 8 different member states. Therefore, the main elements of the EDF model concentrate on: highly attractive projects, wide geographical coverage, large SMEs participation, positive effect on cooperation, full coherence with other EU defence initiatives, contribution to the EU's strategic autonomy, open to third country-controlled subsidiaries, and - last but not least – support to disruptive technologies.

The next call for proposal is expected in the middle of 2023 and can be monitored on the EC portal together with particular tenders, and description of funding and eligibility rules.[15]

3.3 Other funds related to defence

Except for the currently running EDF programme, there are several more means and instruments to support defence research, development and innovation. Some of them have been completed or taken over to other instruments, others are still at the disposal of potential defence-related beneficiaries.

One should bear in mind that access to the EU financing could be received via COSME Programme, which was the EU programme for the Competitiveness of Enterprises and SMEs (small and medium-sized enterprises), running from 2014 to 2020, with a budget of € 2.3bn. An example of activities under this programme is the Call 2017, in the cluster "Go international" in the defence and security sector, whose objective under "Go international" was to support market access of the European defence and security-related clusters and business network organisations to intensify collaboration across borders with other non-defence industrial clusters and to develop and implement joint strategies with non-EU countries in relation to dual-use technologies, products and services. The financial instruments under COSME (i.e. the Loan Guarantee Facility and the Equality Facility for Growth) could be used to finance high-risk SMEs working on defence and dual use.[16]

Connecting Europe Facility (CEF) was a EU funding instrument from 2014 to promote growth, jobs and competitiveness through targeted infrastructure investment at European level. It's dedicated program Single European Sky ATM research (SESAR)finances cooperative projects and studies, with a focus on the European transport infrastructure.[17]

Invest EU brings the European Fund for Strategic Investments and 13 other EU financial instruments under one roof, giving an additional boost to sustainable investment, innovation and job creation in Europe with a new wave (€372 billion) in investments for: sustainable infrastructure; research, innovation and digitisation; social investment and skills; as well as small and medium-sized enterprises.[18]

European Investment Bank (EIB), based on a cooperation agreement of 2018 with the EDA, became a potential financial source – via direct loans, grants and equity – for dual-use R&T projects in cybersecurity and civilian security infrastructure, that are economically, financially, technically and environmentally sound and support the EU defence policy objectives.[19]

European Investment Bank **Source: Palauenc05, Wikimedia Commons, CC3**

In fact, the best single source of information in this regard is the **European Funding Gateway for Defence** website (IdentiFunding) of the EDA with over 20 funding opportunities.[20] It's especially addressed at European level to defence industry, clusters, research and technology organisations, academia, and of course Ministries of Defence or national Armed Forces entities. Going through the Gateway's data, except for the already covered here EU initiatives, the opportunities will include among others: Structural Funds, InvestEU, LIFE, and Erasmus+.

European Structural and Investment Funds (ESIF) are set in the frames of EU Cohesion policy for the years 2021-2027, which require national co-financing and have not been launched for Poland yet due to political and legal constraints. However, in the coming years three tools shall be released for Polish entities and organisations, including the European Regional Development Fund, its 'Interreg' share and the European Social Fund.[21]

The European Regional Development Fund (ERDF) aims at creating jobs, innovation and competitiveness. Taking into account the necessary defence sector perspective, in the ERDF one can fund productive investment projects, projects modernising the defence supply chain, and defence and dual-use activities in research and innovation. On the other hand, **Interreg Europe** is the programme for fostering interregional cooperation with the aim of achieving the European territorial cooperation goal. Interreg Europe can fund the same type of projects of the European Regional Development Fund, but with a focus on cross-border and transnational cooperation.

The third of the cohesion policy tools is the **European Social Fund** (ESF), which can fund projects on key skills and competences in both the defence and dual-use domains, with a focus on human capital, training and skills. The ESF is designed to fund energy projects on climate change adaptation, the environment and resource efficiency, and public administration efficiency and capacity, with the aim of reducing disparities and promoting sustainable development.

Similar environmental approach is enhanced by the LIFE programme for environment and climate action. **LIFE** programme is flexible for funding various opportunities, including pilot, demonstration, best practice and information (awareness/dissemination) projects related to water, waste, energy, the circular economy, chemicals (including REACH – protection of human health and the environment), noise, emissions, etc. With two supplementary tools – the LIFE financial instruments, which is Private Finance for Energy Efficiency (PF4EE) and the Natural Capital Financing Facility (NCFF) – the programme can fund innovative natural capital management pilot projects (NCFF) and energy efficiency investments as well as technical assistance in relation to them (NCFF and PF4EE).[22]

Erasmus+ is another EU programme to take into account. It is addressed at strengthening cooperation between organisations and institutions in Europe, providing means in separate initiatives, e.g.: Learning mobility, Strategic Partnerships and Knowledge Alliances. Therefore, Erasmus+ is the scheme that funds learning mobility for individuals, strategic partnerships and knowledge alliances, which are also applicable in the

NATO Secretary General Jens Stoltenberg

Source: NATO, CC0

field of defence. What's more, the reviewed 2023 Erasmus+ budget brings overall € 4.43 bn to support the education sectors, with specific support for Ukrainian learners and staff.[23]

NATO

Also NATO has set up the €1 billion Defence Innovation Accelerator for the North Atlantic (DIANA) in order to promote innovation in the defence sector, but above all to be prepared for defence and security challenges. DIANA aims to develop dual-use technologies on Emerging and Disrupting Technologies (EDTs), such as artificial intelligence autonomous systems, advanced manufacturing, biotechnologies and quantum technologies. Interestingly enough, the DIANA's pilot programme has been launched already in Spring 2023 and is addressed at various stakeholders, including start-ups, more mature companies, academia, civil and public institutions and test centres.[24] Best reference to the currently available NATO projects is "2023 Collaborative Programme of Work" by the NATO Science & Technology Organisation (STO).[25] The inspiration for the new ones could be based on "Science & Technology Trends 2023-2043. Across the Physical, Biological, and Information Domains".[26]

3.4 Possible consequences for Poland

In view of launching potential Polish-Ukrainian military projects, it's definitely worth considering the EDF means to engage the defence-related small-and-medium enterprises (SME), as well as middle-capitalisation companies (Mid-Caps), and other scientific entities in new research, development endowers and production, as well as consequently define new supply chains for the Polish and Ukrainian Armed Forces. Especially Mid-Caps, like PGZ subsidiaries or Ukroboronprom (esp. Antonow), which can have up to 3 000 employees, in the frames of defence industrial policy balanced development approach, that has been stressed by Poland in the Council conclusions in the last decade, are therefore materialised in the EDF preferences for cross-border cooperation. The EDF is unprecedented, comprehensive instrument covering funding for the whole defence industrial cycle to support European strategic autonomy. In order to use this "financial toolbox" of a set of standardised instruments supporting collaborative research and procurement projects the participation of at least three EU Member States is required, while the consortium could include Ukrainian entities.

Current experience shows that Polish enterprises and research centres have vast possibilities and potential to win EU finances grants and competitions. However, their constraint is still the possibility to find a consortium partner to develop a common project proposal, and also limited international cooperation experience. On top of that there is also a problem of deepening technological gap between Eastern and Western-European defence entities and their research potential and, as a result, slower technological advancement and innovation of the defence research and manufacture. That aspect may hamper participation in some high-tech defence projects (which is visible in terms of member states engaged in such initiatives – vide attached Table 1), but still provides full scope of areas and defence needs specific for Eastern Europe as the Eastern Flank.

Advisable learning tool of how the EU founded projects should proceed and result within the EU's framework programmes for research and innovation is the Community Research and Development Information Service (CORDIS) database, that forms an open-science searcher to stimulate growth across Europe.[27]

Keeping in mind that any defence-related research consortium receiving EU funding shall have a multinational representation, the most effective way to gain cooperation partners, experience and recognisability in the European R&D defence sector is to engage in the works of the EDA technological panels (CapTech), participate in EDF networking events or national information actions (i.e. by NCBR or MoD). EDA funds cooperative defence R&T and capability projects on a continuous basis.

The minimal requirement for project's eligibility is upheld in all EU calls for proposals with at least three entities from at least three Member States or associated countries. However, the results in all cases show strong and rising competition of doubling and tripling the number of proposals for subsequent calls. The final result is also an increase in the average number of participating entities and member states with broad geographical coverage all over the EU, forming the truly European collaboration in the defence sector with attention to inclusiveness and openness of the supply chain. From the EU side, such trend uplifts the quality of proposals, and consequently the level of developed defence capabilities. Moreover, since the EU funds do not cover the acquisition costs, in order to ensure that the EU resources are put to good use, development of common prototypes is funded only when member states intend to buy the final product or use the technology in a coordinated manner. Therefore, no capability is owned by the EU itself.

The EU also provides other sourcing possibilities related to bi- and multilateral defence projects, which should be carefully analysed through the interactive European Funding Gateway for Defence. This information hub selects adequate defence priorities under the Strategic Research Agendas in defence and their Technology Building Blocks, as well as Key Strategic Activities.

Furthermore, taking into account some remarkable commonalities between Central-European entities (i.e. military materiel, mind-set), reasonable step to kick-off transnational defence research and industry cooperation could also be to reconsider the implementation of the Regional Security Support Program 2022 that was adopted in 2015 by the Polish Council of Ministers with the aim to deepen political, military and industrial relations with allied countries: the Visegrad Group (Czech Republic, Slovakia, Hungary), the Baltic states (Lithuania, Latvia, Estonia) as well as Romania and Bulgaria.[28]

3.5 Possible consequences for Ukraine

Ukraine already has access to the projects and programmes coordinated by the EDA based on the Administrative Arrangement between the European Defence Agency and the Ministry of Defence of Ukraine, that was signed on the 7th December 2015.[29] Such agreements are occasionally conducted by the EDA with non-EU members on case-by-case basis to enhance the cooperation possibilities on military technologies developed, although they don't give non-members the right to vote in the frame of the EDA forum. The Annex to the above Arrangement defines the rules of the "participation by the MoD of Ukraine in the EDA Ad Hoc projects and programmes regime applicable to contracts to be let by the EDA". As the initial areas with the potential for cooperation included: Single European Sky, standardisation, logistics (i.e. spare parts and airlift) and training (i.e. helicopter training). Therefore, the EDA – Ukrainian platform seems to be perfect occasion to initiate additional projects of bilateral (Polish-Ukrainian) interest, albeit financed by national MoDs.

Mi-24 Source: Radoslaw Idaszak, Wikimedia Commons, CCO

Moreover, the Association Agreement between the EU and Ukraine has been in force since 1 September 2017.[30] On 28 February 2022, shortly after it was invaded by Russia, Ukraine applied for membership of the EU. Eventually, on 23 June 2022 the Candidate status was granted to Ukraine.[31] It all means that currently Ukraine is eligible to take part in various EU programs, including the Horizon Europe programme for research and innovation, but also participate in the EDF as an associated country. Ukraine is treated currently as a priority partner for the EU, therefore Ukrainian entities are welcome in all sorts of projects.

One of the most tangible areas of cooperation for Polish and Ukrainian entities that currently perfectly fits into the scope of EU financing schema will certainly be disruptive technologies.[32] This particular area is not only essential for the EU but provides synergies with the NATO science and technology trends as seen in the latest report.[33]

President Volodymyr Zelenskyy with NATO Secretary General Jens Stoltenberg at the Vilnius Summit. **Source: NATO, CCO**

Therefore, similar perception of willingness and engagement for Ukraine is on the side of NATO. The cooperation between NATO and Ukraine was initialised already in 2004, and Joined Working Group NATO-Ukraine for Technological Cooperation in the area of Defence was established with the aim to reform the Ukrainian defence industry. The pace of actions was slow but steady. It gave Ukraine access to cooperation with NATO Research and Technology Organisation, to projects on standardisation and codification, as well as others in area of C4, Cyber Defence, Explosive Ordnance Disposal, Logistics Defence or Medical Rehabilitation. In 2015 a roadmap for collaboration in the defence-technical field was signed between NATO and Ukraine, which - among others - forms the basis for Ukrainian entities to take part in NATO Smart Defence initiative.

Table 1. EDF categories of actions and accccepted projects

L.p	Category of Action	Main experience outcome	Indicative EDF budget contribution during 21-27	Projects accepted	Projects topic range	Scope of EU financing, € million
	thematic categories					
1.	DEFENCE MEDICAL SUPPORT, CBRN, BIOTECH AND HUMAN FACTORS	▪ CBRN system of systems (standardisation) and technologies integration ▪ Set of available defence medical countermeasures procured jointly		COUNTERACT European agile network for medical COUNTER measures Against CBRN Threats	The project COUNTERACT will establish a robust and agile network within the EU, capable of developing and deploying medical countermeasures (MCMs) against major CBRN threats. Related PESCO project: European Medical Command (EMC)	49.1
				TeChBiot Surveillance and Reconnaissance Techniques for Chemical and Biological Threats	The project TeChBioT will develop new highly selective and sensitive detectors for the detection and identification of the most volatile chemical or biological warfare agents.	4.3
				MoSaiC Real-time Monitoring and Sampling of CB menaces for improved dynamic mapping of threats, vulnerabilities and response capacities	The project MoSaiC will provide for the real-time monitoring of CBRN events and for innovative sampling technologies to enhance the dynamic mapping of threats, vulnerabilities and response capacities.	4.4
2.	INFORMATION SUPERIORITY	▪ Prototype of a European C2 software suite (contributing to an EU operational headquarter) ▪ Joint procurement of a special operations forces' command post and C2 ▪ EU certified and combat-proven standards for tactical communications and radio interoperability ▪ MALE (medium altitude long endurance) RPAS (remotely piloted aircraft system) prototype, leading to joint procurement ▪ HAPS (high altitude platform systems) prototype, leading to joint procurement ▪ Tactical RPAS prototype, leading to joint procurement ▪ Detect and avoid capabilities for extensive integration in platforms	>10%	5G COMPAD 5G Communications for Peacekeeping And Defense	he project 5G COMPAD will demonstrate the relevance of 5G mobile communications technology in support of sustained information superiority	27.0
				EuroHAPS High altitude platform systems demonstration	The project EuroHAPS will provide airborne technology demonstrators to improve intelligence, surveillance and reconnaissance (ISR) capabilities. Related PESCO project: European High Atmosphere Airship Platform (EHAAP)	43.0
3.	ADVANCED PASSIVE AND ACTIVE SENSORS	▪ Concepts and prototypes of interoperable multi-sensor systems ▪ Consolidated supply chain for optronic detectors and radars ▪ Technological leap in the field of cognitive (adaptable) systems with a focus on radiofrequency (RF)		HEROIC High Efficiency Read Out Circuits	The project HEROIC will provide new advanced electrical components for the next generation IR sensors.	18.0
				ARTURO Advanced Radar Technology in eURОpe	The project ARTURO will provide a solution to fulfil future operational needs based on extended use of emerging technologies for advanced radar technologies in Europe	20.0
4.	CYBER	▪ Creation of two persistent main lines of collaborative actions contributing to the development of European common and/or interoperable tools for: * cyber operations and incident management * information warfare defensive operations and preventive measures ▪ Resilience for cyber physical systems		ACTING Advanced European platform and network of Cybersecurity training and exercises centres	The project ACTING will develop advanced interconnected domain oriented cyber ranges for training and exercises. Related PESCO project: EU Cyber Academia and Innovation Hub (EU CAIH).	16.3
				AInception AI Framework for Improving Cyber Defence Operations	The project AInception will seek to improve cyber defence operations by using AI-based tools and techniques	8.2
				EU-GUARDIAN European framework and proofs-of-concept for the intelliGent aUtomAtion of cyber Defence Incident mAnagemeNt	The project EU-GUARDIAN will create an AI-based solution to automate incident management and cyber defence processes. Related PESCO project: EU Collaborative Warfare Capabilities (ECoWAR)	13.5
5.	SPACE	▪ Joint procurement for integration of PRS (public regulated service) receivers into EU MSs military systems (autonomy/synergy Space/Defence) ▪ Joint procurement of SSA (space situational awareness) capabilities interfaced with EU SST (space surveillance and tracking) ▪ Space-based early warning prototype ▪ Space-based ISR (information, surveillance and reconnaissance) constellation prototype ▪ Potential synergies with the envisioned space connectivity constellation, subject to further analysis	>10%	EPW European Protected Waveform	The project EPW will start the development of a secure waveform standard for future-proof satellite communications.	25.0
				Navguard Advanced Galileo PRS resilience for EU Defence	The project Navguard will strengthen the Galileo PRS resilience through new ground and space-based systems. Related PESCO project: European Radio Navigation Solution (EURAS)	24.4

L.p	Category of Action	Main experience outcome	Indicative EDF budget contribution during 21-27	Projects accepted	Projects topic range	Scope of EU financing, € million
	thematic categories					
6.	DIGITAL TRANSFORMATION	▪ Military operational cloud systems ▪ Shared databases for training, testing and certification of AI systems, and the associated environment to produce, curate and distribute them ▪ Energy-efficient, trustworthy and adaptive AI core technologies for integration into defence systems)		EDOCC European Defence Operational Collaborative Cloud	The project EDOCC will provide a virtual platform to increase collaborative services on the battlefield. Related PESCO project: EU Collaborative Warfare Capabilities (ECoWAR)	40.0
				KOIOS Knowledge Extraction, Machine Learning and other AI approaches for secure, robust, frugal, resilient and explainable solutions in Defence Applications	The project KOIOS will seek to improve AI for military applications, spanning simulation, use-cases, metrics, and real world experiments	10.0
				FaRADAI Frugal and Robust AI for Defence Advanced Intelligence	The project FaRADAI will develop robust artificial intelligence for defence applications.	18.5
7.	ENERGY RESILIENCE AND ENVIRONMENTAL TRANSITION	• Prototype of future green, efficient, resilient, safe and multi-sources energy solutions for the defence sector operating under harsh environmental conditions • Demonstrator of efficient and green engines representative of new architecture and technologies, respectively adapted to each of the following capability: * next generation air combat aircraft * next generation Main Battle Tank (MBT) * next generation naval vessels • Prototype of a technological solution to ensure save reuse of water for military and peace keeping missions • Prototype of green innovative solution for recycling soldier equipment	>5%	INDY Energy Independent and Efficient Deployable Military Camps	The project INDY will develop a strategic roadmap towards future energy independent and efficient deployable military camps. Related PESCO project: Energy Operational Function (EOF)	14.2
				NEUMANN Novel Energy and propUlsion systeMs for Air dominance	The project NEUMANN will study energy aircraft domains, with a focus on energy-efficient propulsion, electrical and thermal systems and management.	48.9
				NOMAD NOvel energy storage technologies usable at MilitAry Deployments in forward operating bases	The project NOMAD will develop next generation electrical energy storage for military forward operating bases. Related PESCO project: Energy Operational Function (EOF	19.7
8.	MATERIALS AND COMPONENTS	▪ Support of supply chains for electronic components ▪ Support of innovation for high-performance and protective materials ▪ Certification of technologies for manufacturing and maintenance		ECOBALLIFE Research in eco-designed ballistic systems for durable lightweight protection against current and new threats in platform and personal applications	The project ECOBALLIFE will use new technologies to improve protection for soldiers and vehicles.	10.0
				AGAMI_EURIGAMI European Innovative GaN Advanced Microwave Integration	The project KOIOS will seek to improve AI for military applications, spanning simulation, use-cases, metrics, and real world experiments	24.6
9.	AIR COMBAT	• Critical components and technologies for next generation fighter systems • EU standards for collaborative air combat • Prototype of next generation rotorcraft, leading to joint procurement • Joint procurement of an airborne electronic warfare capability	>10%	EPIIC Enhanced Pilot Interfaces & Interactions for fighter Cockpit	The project EPIIC will focus on new air power capabilities and seek to ensure the Air dominance of the European defence forces. Related PESCO project: Air Combat	75.0
				EICACS European Initiative for Collaborative Air Combat Standardisation	The project EICACS will focus on interoperability for European air forces' mission management	74.8
				ENGRT EU Next Generation Rotorcraft Technologies Project	The project ENGRT will focus on the next generation of EU military rotorcrafts	40.0
10.	AIR AND MISSILE DEFENCE	• Prototype of endo-atmospheric interceptor • Prototype of counter UAS, leading to joint procurement	>5%	EU HYDEF European Hypersonic Defence Interceptor	The project EU HYDEF will define the concept for a European Interceptor to achieve the highest maneuverability and capability to respond to high velocity threats. Related PESCO project: Timely Warning and Interception with Space-based TheatER surveillance (TWISTER)	100.0

L.p	Category of Action	Main experience outcome	Indicative EDF budget contribution during 21-27	Projects accepted	Projects topic range	Scope of EU financing, € million
	thematic categories					
11.	GROUND COMBAT	▪ Joint development and procurement of a different set of vehicles and integration of technologies for vehicles upgrades ▪ Contribution to future MBT and other armoured vehicles development ▪ BLOS (Beyond the line-of-sight) capability jointly procured ▪ Development of a long-range indirect fire demonstrator ▪ Unmanned ground systems jointly developed and ready to procure ▪ Contribution to enhanced connectivity and interaction among land platforms (manned/unmanned, mounted/dismounted) and initial integration of collaborative land combat capabilities into national platforms	>10%	MARSEUS Modular Architecture Solution for EU States	The project MARSEUS will develop a collaborative close combat architecture enhancing existing missile systems with a Beyond-Line-Of-Sight capability. Related PESCO project: EU Beyond Line Of Sight (BLOS) Land Battlefield Missile Systems (EU BLOS)	25.0
				FAMOUS2 MEuropean Future Highly Mobile Augmented Armoured Systems 2	The project FAMOUS2 will enhance all-terrain vehicles, light armoured vehicles and main battle tanks through developments and upgrades	94.8
				NEWHEAT New European Warhead Technologies	The project NEWHEAT will improve the performance of conventional shaped charge by integrating new high explosive, new liner materials and new geometries	10.0
				COMMANDS Convoy Operations with Manned-unMamneD Systems	The project COMMANDS will develop capabilities for agile, intelligent and cooperative manned and unmanned land systems. Related PESCO project: Integrated Unmanned Ground System (UGS)	24.8
12.	FORCE PROTECTION AND MOBILITY	▪ Standardisation of European soldier systems and systems jointly procured (e.g., equipment, interconnection) ▪ Contribution to improvement of soldiers' situational awareness, decision-making, effective engagement, operation in Global Navigation Satellite System (GNSS) denied environments, and teaming with unmanned systems through enhanced Soldier Systems ▪ Contribution to a future medium size tactical cargo aircraft development		ACHILE Augmented Capability for High end soLdiErs	The project ACHILE will develop highly innovative solutions for a next generation Dismounted Soldier System. Related PESCO project: EU Collaborative Warfare Capabilities (ECoWAR)	40.0
				SDMMS Secure Digital Military Mobility System	The project SDMMS will develop a secure digital information system in support of Military Mobility.	9.1
13.	NAVAL COMBAT	▪ Joint procurement of a modular and multirole patrol corvette class ▪ First ship of a medium-size semi-autonomous surface vessel class, including different mission modules, leading to joint procurement of the class and including the development of standards related to automation ▪ Joint procurement and integration in different platforms of a naval collaborative surveillance capability ▪ Development activities leading to a naval collaborative engagement capability ▪ Development of standards related to smart ships and digital transformation	>10%	EPC European Patrol Corvette	The project EPC will focus on the initial phase of a European innovative, modular, flexible, interoperable, green, multirole vessel, enabling the European navies to face the 21st century challenges. Related PESCO project: European Patrol Corvette	60.0
				EDINAF European Digital Naval Foundation	The project EDINAF will provide a European digital ship reference architecture, integrating the systems onboard altogether in order to achieve vessels fastest reaction and enhanced capabilities.	29.0
				dTHOR Digital Ship Structural Health Monitoring	The project dTHOR will develop the next generation of a predictive Ship Structural Health Monitoring system.	14.5
14.	UNDERWATER WARFARE	▪ Prototype of a semi-autonomous modular mine-countermeasures suite ▪ Prototype of an unmanned anti-submarine warfare solution ▪ Development of an advanced underwater observation and communication system for long ranges ▪ Development of swarm systems for multiple mission types				
15.	SIMULATION AND TRAINING	▪ Foster innovation and cooperation for stakeholders in the defence modelling and simulation (M&S) domain ▪ Create an ecosystem in simulation ▪ Prepare and align the technical solutions to facilitate joint procurements				

L.p	Category of Action	Main experience outcome	Indicative EDF budget contribution during 21-27	Projects accepted	Projects topic range	Scope of EU financing, € million
	thematic categories					
16.	**DISRUPTIVE TECHNOLOGIES**	▪ Demonstrator of a medium calibre electromagnetic artillery system (contributing to long range indirect fire capabilities' development) ▪ Other disruptive technologies, including quantum, metamaterials and AI techniques for defence applications	**4% – 8%**	**ROLIAC** Robust and Light AM components for military systems	The project ROLIAC will focus on new materials and technologies for additive manufacturing of lightweight parts of defence equipment.	**4.0**
				ENLIGHTEN European Non-Line-of-Sight Optical Imaging	The project ENLIGHTEN will seek to develop next-generation electro-optical (EO) sensing devices for operational effectiveness.	**8.4**
				ADEQUADE Advanced, Disruptive and Emerging QUAntum technologies for DEfense	The project ADEQUADE will focus on breakthrough in quantum technologies for defence.	**27.4**
				iFURTHER High Frequency Over The Horizon Sensors' Cognitive Network	The project iFURTHER will address new technologies for air and sea long-range detection.	**11.0**
17.	**INNOVATIVE DEFENCE TECHNOLOGIES (SMEs)**			**ALADAN** Ai-based Language technology development framework for Defence ApplicatioNs	The project ALADAN will develop an AI-based language solutions for defence applications	**3.2**
				ABITS Advanced Biometrics In Training and Simulation	The project ABITS will develop an in-door tactical training solution using advanced biometrics.	**2.2**
				HYBRID Hydrogen Battlefield Reconnaissance and Intelligence Drone	The project HYBRID will develop a long endurance electric hydrogen fuel cell-powered drone.	**3.1**
				SPRING Space Response to Risk & Integration with Ground segment	The project SPRING will develop an integrated solution for automated response to threats to increase the safety and reactivity of military space systems.	**3.7**
				SHOLFEA SHOulder Launched Family for European Armies	The project SHOLFEA will develop a family of shoulder-launched missile systems addressing the operational needs of future infantry units.	**2.8**
				RFSHIELD RF Interference Removal for Military Services based on Spaces Link	The project RFSHIELD will develop a solution to protect the Satellites Communication services	**3.4**
				ALTISS Highly Automated Swarm of Affordable ISR Long Endurance UAVs for force protection	The project ALTISS will provide improved ISR (Intelligence, Surveillance and Reconnaissance) capacity through an affordable resilient UAVs (Unmanned Air Vehicle) swarm	**3.2**
				NAUCRATES Microsatellite for Geostationary Orbit Surveillance and Intelligence	The project NAUCRATES will work on the demonstrator of a satellite intended for the optical intelligence of Geostationary Earth Orbit (GEO) resident objects. Related PESCO project: European Military Space Surveillance Awareness Network (EU-SSA-N)	**4.0**
				POWERBACK Novel 3D heterogeneous integration for future miniaturized power RF Transceiver front ends	The project POWERPACK will develop disruptive technologies for miniaturised Radio Frequency Identity (RF) chips for high frequency and high-power operation.	**3.5**
				P2P-FSO Platform to Platform Free Space Optical link	The project P2P-FSO aims at the provision of a free space optical point-to-point communication system.	**2.4**
				SMiEQ Secure Microcontroller with Embedded Quantum Random Number Generator	The project SMiEQ will prototype a secure microcontroller with an embedded quantum random number generator	**3.5**

L.p	Category of Action	Main experience outcome	Indicative EDF budget contribution during 21-27	Projects accepted	Projects topic range	Scope of EU financing, € million
	thematic categories					
				HIDRA High Instantaneous Dynamic Range Direct RF sampling modular chiplet Architecture	The project HIDRA will aim at the provision of a modular chiplet architecture for Software Defined Radio.	4.0
				IntSen2 Proactive automatic imagery intelligence powered by artificial intelligence exploiting European space assets	The project IntSen2 will use Artificial Intelligence to develop a concept of application for Imagery intelligence (IMINT).	3.3
				LODESTAR Live operational data enhancement for situational awareness through augmented reality	The project LODESTAR will integrate augmented reality and artificial intelligence in modern, highly efficient soldier systems.	3.7
				Mini-BOT Miniaturized Board-mountable Optical Transceiver for high data rate Military Satellite Communications	The project Mini-BOT will establish the first European supply chain of high-performance optical transceivers.	3.4
				SEAWINGS Sea/Air Interphasic Wing-in-Ground Effect Autonomous Drones	The project SEAWINGS will develop a new class of military surveillance drones to operate in the sea/air interface.	3.9
				Nano-SHIELD	The project Nano-SHIELD will develop the next generation of nanofibers for Chemical-Biological-Radiological-Nuclear (CBRN) protection	4.0
				Q-SiNG Quantum-based Simultaneous inertial Navigator and vector Gravimeter	The project Q-SiNG will provide a navigation system demonstrator for GNSS-denied areas.	3.9
				FIBERSENSE Using fiber optical cables for maritime situational awareness	The project FIBERSENSE will focus on and advance the Distributed Acoustic Sensing (DAS) technology.	3.4
				FACELIFT Fluidic Actuators for Control of stealth alrcraFT	The project Facelift will improve the strategic surveillance capability, survivability and operational resilience of future stealth aircrafts.	3.5
				AMLTD Additive Manufacturing of Lightweight Laser Target Designator	The project AMLTD will develop a miniature Laser Target Designator.	2.9
				HEGAPS Hybrid Energy Grid and Propulsion System	The project HEGAPS will work on a cyber-physical system to coordinate multiple assets.	4.0
				POWERFLEX Smart, Heterogeneous Technological Platform Extending the Power and Frequency Limits of Flexible Nanoelectronics	The project POWERFLEX will work on new flexible antennas based on new and advanced materials.	3.5

Source: own research based on the European Commission data on The European Defence Fund site: (https://defence-industry-space.ec.europa.eu/eu-defence-industry/european-defence-fund-edf_en).

3.6 Conclusions

Placing significant emphasis on research and development activities in the EU and connecting their major directions with PESCO initiatives seem to be not only the current necessity in the European strategic autonomy policy, but above all the stimulus for transborder military cooperation in the Central Eastern Europe.

International community is especially in favour of extending cooperation with Ukraine and Ukrainian entities in the face of the outrages done by Russia. At that point all sorts of reflection and support will lead to involve Ukraine into EU and NATO processes and programmes,[34] including defence industrial assistance and joint R&T projects. With the constant growth of EU funding for defence R&D, the above analysis shows new ways and windows to finance military-related projects. Polish entities may become a leading example in engaging adequate cooperation forms.

Sources

[1] "Common security and defence policy", Fact Sheets on the European Union – European Parliament, March, 2023, https://www.europarl.europa.eu/factsheets/en/sheet/159/common-security-and-defence-policy.

[2] Bordin, G., Hristova, M. and Luque Perez, E. editor(s), Security and defence research in the European Union: a landscape review, EUR 29864 EN, Luxembourg , Publications Office of the European Union, 2019, ISBN 978-92-76-11442-0, doi:10.2760/100724, JRC117742.

[3] EDA - https://eda.europa.eu/; Capability Technology Areas - https://eda.europa.eu/what-we-do/research-technology/capability-technology-areas-(captechs); Research & Technology https://eda.europa.eu/what-we-do/research-technology

[4] "Hub for EU Defence Innovation Established within EDA", European Defence Agency, May 17, 2022, https://eda.europa.eu/news-and-events/news/2022/05/17/hub-for-eu-defence-innovation-established-within-eda.

[5] "European Defence Action Plan", European Commission, July, 17, 2017, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=LEGISSUM:4298898.

[6] PESCO - https://www.pesco.europa.eu/

[7] "Coordinated Annual Review on Defence", European Defence Agency, n.d., https://eda.europa.eu/what-we-do/EU-defence-initiatives/coordinated-annual-review-on-defence-(card)

[8] Regulation (EU) 2021/697 of the European Parliament and of the Council of 29 April 2021 establishing the European Defence Fund and repealing Regulation (EU) 2018/1092, L 170/149, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32021R0697&from=EN.

[9] "Preparatory Action on Defence Research (PADR)", European Commission, n.d., https://defence-industry-space.ec.europa.eu/eu-defence-industry/preparatory-action-defence-research-padr_en.

[10] "European Defence Industrial Development Programme (EDIDP)", European Commission, n.d., https://defence-industry-space.ec.europa.eu/eu-defence-industry/european-defence-industrial-development-programme-edidp_en.

[11] Justification for Polish projects shall be in line with the current version of "Priority research directions in the Ministry of National Defence for the years 2017-2026", https://dna.wat.edu.pl/images/dna/fundusze-krajowe/priorytetowe_kierunki_2017-26.pdf. In the area of technique and defence technologies the following seven priorities are set: information and network technologies; sensors and observation; precision weapons and armaments; unmanned autonomous systems; survival and protection on the battlefield; modern materials, including high-energy and intelligent materials; breakthrough technologies.

[12] „Europejski Fundusz Obronny 2021", Ministerstwo Obrony Narodowej, n.d., https://www.gov.pl/web/obrona-narodowa/europejski-fundusz-obronny-2021; „Europejski Fundusz Obronny 2022", Ministerstwo Obrony Narodowej, n.d., https://www.gov.pl/web/obrona-narodowa/e.

[13] Among others: National Security Strategy of the Republic of Poland, 12.05.2020; "Priority research directions in the Ministry of National Defence for the years 2017-2026".

[14] "The European Defence Fund (EDF)", European Commission, n.d., https://defence-industry-space.ec.europa.eu/eu-defence-industry/european-defence-fund-edf_en;
"European Defence Fund Indicative multiannual perspective 2021-2027 (Releasable version of Annex 2 of Commission Implementing Decision C(2022)3403 dated 25 May 2022)", Brussels, European Commission, 25.05.2022, https://defence-industry-space.ec.europa.eu/system/files/2022-05/EDF%20Indicative%20multiannual%20perspective.pdf.

[15] "European Defence Fund 2021 Calls for Proposals – Results", Defence Industry and Space, July 20, 2022, https://defence-industry-space.ec.europa.eu/funding-and-grants/calls-proposals/european-defence-fund-2021-calls-proposals-results_en;
Search Funding & Tenders - https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-search;callCode=null;programCode=EDF;programmePeriod=2021%20-%202027;typeCodes=1,0;freeTextSearchKeyword=;

[16] "COSME- Europe's programme for small and medium-sized enterprises", Internal Market, Industry, Entrepreneurship and SMEs, n.d., https://single-market-economy.ec.europa.eu/smes/cosme_en.

[17] "Connecting Europe Facility", Innovation and Networks Executive Agency, December 22, 2022, https://wayback.archive-it.org/12090/20221222151902/https:/ec.europa.eu/inea/en/connecting-europe-facility.

[18] "Invest EU", Internal Market, Industry, Entrepreneurship and SMEs, n.d., https://single-market-economy.ec.europa.eu/access-finance/investeu_en.

[19] "Loans", European Investment Bank, n.d., https://www.eib.org/en/products/loans/index.htm.

[20] "EU Funding – European Funding Gateway for Defence (EFGD)", European Defence Agency, https://eda.europa.eu/eufunding.

[21] Inforegio – "Available budget of Cohesion Policy 2021-2027", European Commission, n.d., https://ec.europa.eu/regional_policy/funding/available-budget_en.

[22] "Programme for Environment and Climate Action (LIFE)", European Commission, https://commission.europa.eu/funding-tenders/find-funding/eu-funding-programmes/programme-environment-and-climate-action-life_en.

[23] "Erasmus+", European Commission, n.d., https://erasmus-plus.ec.europa.eu/pl.

[24] "NATO approves 2023 strategic direction for new innovation accelerator", North Atlantic Treaty Organization (NATO), December 12, 2022, https://www.nato.int/cps/en/natohq/news_210393.htm.

[25] NATO Science & Technology Organization - https://www.sto.nato.int/Pages/default.aspx

[26] Dale F. Reding et al., STO, Science & Technology Trends 2023-2043. Across the Physical, Biological, and Information Domains. Volume 1: Overview, Brussels, Belgium, NATO Science & Technology Organization, 2023, https://www.nato.int/nato_static_fl2014/assets/pdf/2023/3/pdf/stt23-vol1.pdf; Dale F. Reding et al., STO, Science & Technology Trends 2023-2043. Across the Physical, Biological, and Information Domains. Volume 2: Analysis, Brussels, Belgium, NATO Science & Technology Organization, 2023, https://www.nato.int/nato_static_fl2014/assets/pdf/2023/3/pdf/stt23-vol2.pdf)

[27] CORDIS, n.d., https://cordis.europa.eu.

[28] Resolution No. 173 of the Council of Ministers of September 22, 2015 on establishing the „Region Security Support Program 2022" - https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WMP20150001019

[29] Administrative Arrangement between the European Defence Agency and the Ministry of Defence of Ukraine, 7th December 2015 - https://eda.europa.eu/docs/default-source/documents/aa---eda---ukraine-mod-07-12-15.pdf

[30] Council Decision (EU) 2017/1248 of 11 July 2017 on the conclusion, on behalf of the European Union, of the Association Agreement between the European Union and the European Atomic Energy Community and their Member States, of the one part, and Ukraine, of the other part, as regards provisions relating to the treatment of third-country nationals legally employed as workers in the territory of the other party, L 181,
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L:2017:181:TOC

[31] Conclusions of the European Council, June 24, 2022, EUCO 24/22, https://www.consilium.europa.eu/media/57442/2022-06-2324-euco-conclusions-en.pdf

[32] Slyusar V., Sotnyk V.V., Kupchyn A., "Disruptive technologies in the defense sphere of Ukraine. Weapons and military equipment", 1(28), (2021), 13-23. https://www.researchgate.net/publication/348185959_Disruptive_technologies_in_the_defense_sphere_of_Ukraine.

[33] D.F. Reding, J. Eaton, Science & Technology Trends 2020-2040 Exploring the S&T Edge, NATO Science & Technology Organization, Brussels, Belgium, NATO Science & Technology Organization, 2020, https://www.nato.int/nato_static_fl2014/assets/pdf/2020/4/pdf/190422-ST_Tech_Trends_Report_2020-2040.pdf.

[34] D.F. Reding, J. Eaton, Science & Technology Trends 2020-2040 Exploring the S&T Edge, NATO Science & Technology Organization, Brussels, Belgium, NATO Science & Technology Organization, 2020, https://www.nato.int/nato_static_fl2014/assets/pdf/2020/4/pdf/190422-ST_Tech_Trends_Report_2020-2040.pdf.

4

Security of the Polish-Ukrainian military cooperation

Andrzej Kozłowski

The Polish-Ukrainian cooperation of military industries might bring great opportunities and chances, but considering their sensitive nature they are also very vulnerable to many risks coming both from the traditional hostile actions as well as digital ones. Planning any mutual activity must take into account the possible threats and prepare to counter them.

4.1 Threats landscape

The military cooperation between Ukraine and Poland may significantly strengthen Ukrainian capabilities on the battlefield through the delivery of new equipment and ammunition but also vital repairs of the damaged military materiel. In short, it could play a vital role in improving the logistics of the Ukrainian army and may be decisive on the battlefield. Poland could also benefit from such cooperation. It could be a valuable lesson to the Polish Armed Forces and Polish military industry about the real wartime tests of the military equipment, logistics and maintenance. Therefore, such cooperation and all the initiatives within it have become a natural target of any Russian hostile activity. Russian Intelligence in the past successfully conducted actions both in traditional and cyber domain and their capabilities and determination should not be disrespected. To better understand possible threats, which may impede the cooperation of military industry, the past cases of the attacks should be analysed in details.

4.2 Russian sabotage actions against military facilities in the past

In 2015 the sky over Iganovo in Bulgaria burst into fiery shades of red and orange as the result of the explosions at the Vazoc Machine-Building Plant, where anti-tank munitions, anti-aircraft missiles and other weapons were being manufactured. Three weeks later

FSB Officers

Source: Andrey Stenin, RIA Novosti, Wikimedia Commons, CC3 further explosions damaged the military complex even further. However, it was not the first time that such an attack took place in Bulgaria. In 2014 there were four other explosions at various sites in Bulgaria, where weaponry was being manufactured. In the same year, an explosion took place in the Czech Republic. In both cases the Russian military intelligence was blamed.[1] The case of Bulgaria was at that time especially vital as Ukraine was desperately looking for weapons to defend against Russian attacks in Luhansk and Donetsk oblasts in 2014. However, these examples show that Russian military intelligence was capable of conducting sabotage actions against military entities in various NATO and EU countries. The same scenario might be repeated now, especially that Russia tries to disrupt the weapon deliveries to Ukraine and might risk a lot to achieve its aims.

In Europe, since the outbreak of the large scale invasion there were security incidents, which might be classified as acts of sabotage. After the Kerch bridge bombing, which is connecting Crimea with Russia, trains in northern Germany were stopped after the communication cable was sabotaged. The German Minister for Transport Voler Wissing said that it was a clearly targeted and malicious action. Denmark also suffered from a mysterious incident, when the island of Bornholm was cut off from electricity after the cable from Sweden was damaged. Additionally, Internet cables were damaged in the south of France at three locations simultaneously. According to the Cloud security company the cables were cut. Norway also informed about suspicious drones near its energy critical infrastructure, airfields and military facilities, where more violations were recorded in one month than for the whole previous year.[2]

German train

Source: Rolf Heinrich, Wikimedia Commons, CC3

4.3 Growing Russian activity in Poland

Russian hostile activity has risen not only in Western Europe but is also noticeable in Poland. There have already been attempts to collect information about logistic points such as Rzeszów airport, which has been converted into an international logistic hub – a vital point for Ukrainian aid and near railways and most important transport routes in Podkarpackie province, where surveillance cameras were planted. Six people were detained in this case and they were also accused of not only conducting surveillance activity but also preparing sabotage plans.[3] However, they are not the only people arrested in Poland on suspicion of spying for Moscow. A Russian citizen, who was allegedly linked to historical reconstruction groups where he tried to establish relations with Polish military personnel was arrested earlier. Likewise, the Spanish national of Russian origin, who was detained in Przemysl and was later identified as the agent of Russia's Military Intelligence Agency. Also, a local clerk in Warsaw Registry Office was arrested.[4] Another dangerous incident happened near the port of Gdansk, when three allegedly Spanish divers were rescued by Polish Maritime Search and Rescue Services. Officially they were looking

Rzeszów Airport **Source: Rzeszów Airport, Wikimedia Commons, CC3**

for amber, but the circumstances of their search which was done during night were suspicious. What is more, they did not have relevant documents, the sea was cold and stormy and not favourable for such an expedition. The region, where they were found is very close to the critical infrastructure Naftoport, which is responsible for management of crude oil shipment and deliveries.[5] All these examples perfectly show the growing activity of Russian and Belarusian special services, which may also want to hit any potential Polish-Ukrainian military entities.

4.4 Relevant security measures

In order to avoid such situations, the Polish and Ukrainian governments and the military companies that engage in mutual security and defence projects need to act and enforce strict security measures. The potential entities of military cooperation should have an additional protection by counter-intelligence officers but also areas, where they are set up could be isolated. Poland has already introduced a 200 meters no-go zone areas near the critical infrastructure in the Polish city of Swinoujscie. Such measures might be also introduced in key areas of Polish-Ukraine military industry cooperation.[6] However, these security tools might be problematic and lead to protests of local population and therefore they should not be treated as a universal solution. The increase of security apparatus in and near facilities seems to be less problematic. It has happened in the case of workshop belonging to state-owned Polish Armaments Group, which is secured by the Polish Internal Security Agency. In this facility more than 400 mechanics and engineers are working on repairing Polish-made AHS Krab howitzers.[7]

The Świnoujście LNG terminal **Source: Radosław Drożdżewski, Wikimedia Commons, CC4**

In increasing security of key entities, the aspect of building awareness among local population is especially vital. Nobody knows the environment better than the local people and they can easily spot new individuals, who might be covert Russian or Belarusian members of Secret Services. The self-aware local population with knowledge about the potential threats and an easy way of contacting the adequate services such as police is a key and an important element of building a resilient society. Unfortunately, it is still not on an adequate level even among specialised units, which was demonstrated in the case of Spanish scuba-divers. They were easily released without confirming their identities. Later it was not possible to find them.[8] Such a situation cannot be repeated in the future and all members of the security apparatus and society need to understand that Poland is neighbouring with two lethal enemies: Belarus and Russia and plays a key role in helping Ukraine win the war against Russia.

The last, though not the least important, security measure, involves the monitoring of Internet and social media particularly Telegram groups, where there might be information about secret military facilities and plans of potential attacks. Probably, the Polish Intelligence is conducting such activities, but the effective exchange of information with companies involved in Polish-Ukrainian military cooperation is also necessary. It could help prevent sabotage actions but also might indicate that there is a leakage of information from the facility and it should be checked again. The last leakage of Pentagon secret paper shows the importance of monitoring the Internet in search for possible sensitive information.

4.5 Cyber-threat landscape

The potential cooperation between the Ukrainian and Polish industry might be hampered not only in the physical world but also in cyberspace. There is a long history of successful cyberattacks against military facilities, which are a very interesting target from the perspective of state hackers. The military companies were in the past targeted by hackers mainly because it was easier to hit them than hacking military units or even ministries of defence or other state institutions responsible for defence and security, mainly because of the lower standards of cyberdefence.

F-35, Source: Donald R. Allen U.S. Air Force, Wikimedia Commons, CC0

V-22 **Source: FOX 52, Wikimedia Commons, CC4**

One of the most long-term effective espionage campaigns was the hacking of the American military giant Lockheed Martin by Chinese hackers. The campaign lasted for a couple of years in the first decade of the 21st century and Chinese hackers were able to obtain information about the F-35 secret program, which was crucial in building their own 5-generation fighter.[9] Other cyber espionage operations conducted by China allowed it to illegally obtain information about other weapon systems such as THAAD missile air defence system, Patriot missile, Navy's Aegis ballistic-missile defence system, V-22 Osprey aircraft, Black Hawk helicopter and Littoral Combat Ships. Almost all of these systems are one of the newest American weapon platforms and are recognised as the crucial component in potential American-Chinese confrontation.[10] The American military industry was not the only one affected. In 2014 Israeli defence contractors such as Elisra Group, Israel Aerospace Industries and Rafael Advanced Defence were hacked by presumable Chinese hackers, who were able to steal hundreds of documents including the design of Israeli rocket system, Iron Dome systems and others.[11]

There are many potential factors why Kremlin might use hackers to breach the defences of military industry entities. Russian hackers might want to plant spyware in networks of the companies to get knowledge about such details as the size of production, what kind of equipment is prioritised and also to get to know information about the ways of transporting this equipment to Ukraine. On the other hand, they may also collect information about weak points of the produced equipment and in that way help other military branches effectively neutralise it or can also collect information about the employees to later blackmail them.

Since the Russian large scale invasion of Ukraine, U.S cybersecurity agencies informed about the 800% increase of cyberattacks and president Biden warned about the risk of detrimental cyberattacks for American companies.[12] Also, CERT Polska informed about the 35% increase of cyberattacks in 2022 in comparison to the previous year and was linked with the war in Ukraine.[13] Naturally, Ukraine was deeply impacted too, with the number of attacks increasing tenfold in the first months of 2022.[14]

Bayraktar TB2 Source: Bayhaluk, Wikimedia Commons, CC4

It is obvious that Russia has been using cyber capabilities to harm Ukrainian allies, as they are an effective measure under the threshold of war. In the early stages of the Russian large scale invasion the Bayraktar TB2 drones were effectively destroying Russian armour columns and probably this fact drove the Russian hackers to infiltrate IT systems and networks of the drones' producer, the Turkish military company Baykar.[15] The details of this incident are unknown but in the further phase of the war Bayraktar TB2 drones were rather absent.[16] There is no evidence that hackers' actions somehow impacted this situation but such a scenario could not be ruled out. Russian hackers might acquire vital information about the drones' weakness or the way how to effectively disrupt them.

It has not been the only cyberattack since the large scale invasion on Ukraine against military industry, which was noticed. German military manufacturer Rheinmetall business unit was hit by cyberattacks, but they were repelled and the company's defence division responsible for military vehicles, weapons and ammunition production remained untouched. Probably the Russian hacker group Killnet was behind it as it had communicated on Telegram about the possible cyberattack. The timing of the attack was not accidental, as at that time Germany was talking about the construction of a new tank factory in Ukraine and Rheinmetall is also a key supplier of Leopard tanks, Marder infantry fighting vehicles, and 155mm calibre artillery shells.[17]

Killnet also launched DDoS attacks against Lockheed Martin, which produces very effective HIMARS systems but these attacks did not pose a serious threat.[18] Also, there is a vital lesson from the hack, which probably happened in the earlier phase of war in Ukraine in 2015, when Russian hackers allegedly breached the security of a Ukrainian application, which was used to better coordinate the artillery fire. The successful operation of Russian hackers allowed Russian forces to easily track Ukrainian artillery and eliminate them.[1] These examples perfectly show that hacking military facilities happened many times in the past but also prove that Russia has the cyber capabilities to conduct even the most sophisticated cyberoperations. Therefore, the risk of cyberattacks against any projects of mutual Ukraine-Polish military cooperation must be considered as high.

4.6 Measures to protect against cyberattacks

Before the Russian large scale invasion on Ukraine, Poland introduced a Charlie-CRP alert,[2] which signifi-

HIMARS Source: General Staff of the Armed Forces of Ukraine, Wikimedia Commons, CC4

Cybersecurity **Source: Pixabay, CC0**

cantly raised up the level of Polish cyber-defence. In practice this alert obliged those responsible for system security to boot security procedures, put administration on round-the-clock duty and increase awareness of workers in critical infrastructure and public administration. All companies, which take part in Polish-Ukrainian military cooperation initiatives should comply with the higher standards of security imposed by the Charlie CRP alert.

The cooperation with the CERTs', which are the backbone of the Polish cybersecurity system is crucial. The smooth and fast exchange of information about the latest threats such as new malware or innovative techniques of attack is important. However, the cooperation must also include the Ukrainian CERT's, which are on the frontline of digital fight with Russian hackers. The cooperation might be much wider and also liaise with cyber security threat Intelligence Service providers to better understand possible risks and threats.[19]

Humans are the weakest element of the cybersecurity chain – this statement is repeated over and over, but hackers still exploit the employees' errors, lack of knowledge and sometimes just tiredness. In such sensitive projects, people will be naturally targeted by phishing and other techniques and tactics. Therefore, regular trainings are necessary as well as phishing drills checking the preparation of the employees. People need to be aware of potential risk posed by phishing but also by fraudulent websites.

Potential employees of the Ukrainian-Polish industry military cooperation should also be taught about data they post on social media and in broader Internet. They should limit the amount of information they publish especially about their work. Social media are the natural environment for all Intelligence Services, which are collecting information about potential targets. They might be used for spearphising emails but also to simply blackmail people and force them for example into cooperation.

What is more, the adequate security equipment such as security keys, isolation of high-risk systems and deletion of unused or expired accounts should become a standard procedure. Ports and protocols, which are not essential for business purposes should be disabled.[20] It is also important to check if all licenses and programs are up-to-date and data is regularly backed up. Naturally, the organisation networks must be protected by antivirus/antimalware tools, which are regularly updated.[21] Implementing an effective security monitoring is also important to increase the preparedness for potential cyberattacks as the time between initial compromisation and launch of malware is now much faster

[1] American company CrowdStrike published a report claiming that Russian groups used a malware on Android devices to track and target Ukrainian artillery units from 2014 to 2016. (Dustin Volz, Russian hackers tracked Ukrainian artillery units using Android implant: report, https://www.reuters.com/article/us-cyber-ukraine-idUSKBN14B0CU)

[2] This alert is introduced when events suggest a probable subject of an attack targeting public security, the security of Poland, or the security of another country, creating a potential threat to Poland,". CHARLIE can also be introduced when there is credible and confirmed information about a planned event of a terrorist nature.

and is counted in days rather than months. Therefore, the time detection and response to any breach must be prepared too.[22]

The organisations should also empower Chief Information Security Officers (CISO) and should step back from the traditional balance between costs and operational risks to the business. Taking into account that the threat environment is heightened for the entities engaged in Polish-Ukrainian military industry cooperation, the CISOs should be included in the decision-making process for risk to make sure that the management understands that cybersecurity is a top priority and the investment in it could not be delayed any further.[23]

Entities engaged in Polish-Ukrainian military cooperation should also prepare to handle and resolve attacks, which will break their defence lines. They need to prepare contingency plans for such incidents and how to communicate them. The updated response plans are also vital in minimising the damage of the incident. Simply, they need to be prepared for the worst-case scenario. They should also include not only security and IT teams, but also senior business leadership and Board members. In addition, the plans should be tested among all the interlocutors mentioned above in order to prepare the organisation to manage a major cyber incident not only in one organisation but also in other entities, which are involved in Polish-Ukrainian military cooperation.[24] The rapid identification and response for any security breach might be crucial in minimalising harmful effects of cyberattacks and denying potential aggressors.

4.7 Conclusions and recommendations

Polish-Ukrainian military cooperation will be a target for Russian and Belarusian Secret Services both in the kinetic and cyber field. In the past they proved that they were able to conduct advanced espionage and disruptive operations against military infrastructure in NATO and EU countries and any entities of Polish-Ukrainian military cooperation automatically might have been a target of Russian Secret Services.

Polish military industry must understand that engagement in the military cooperation with Ukraine might end in the risk of nation-backed cyberattacks on IT systems and infrastructure as well as physical sabotage. It will not be working in peaceful terms but rather in a highly risky environment.

The awareness of this threat landscape requires incorporating security by design in all mutual initiatives. Security must be projected and implemented before the start of the project rather than during it.

The security tools to protect against sabotage and any other hostile action in physical world must be introduced and include increasing security personnel and monitoring apparatus. In some cases, also introducing 200 metres no-go zones might be a good solution but this measure should not be overexploited.

Building awareness among local population is also a very good solution as local people mostly have the best insight and knowledge about local areas and can easily detect any potential hostile behaviours.

It is significant to also introduce the necessary protective measures in cyberspace, which include the adoption of the best and well known measures to increase cyberdefence of the companies.

Building up the counterintelligence awareness among the employees of such projects and place is critically important and should also include cyber-hygiene.

Last but not least, the effective monitoring of the Internet and especially social media might lead to early detection of any possible threats to the key facilities of the Polish-Ukraine military cooperation.

Ukrainian D-20 howitzer **Source: The Ministry of Defense of Ukraine, Wikimedia Commons, CC2**

Sources

1 Boris Mitov, and Ivan Bedrov, “Data Shows Alleged Russian Agents In Bulgaria Around Time Of Arms-Depot Blasts”, Radio Free Europe/ Radio Liberty, April 22, 2023, https://www.rferl.org/a/russia-bulgaria-arms-depot-explosions-gru-agents-gebrev/31217945.html.
2 John Psaropoulos, “Europe awakens to the threat of sabotage by Russian agents”, Al Jazeera, January 17, 2023, https://www.aljazeera.com/news/2023/1/17/europe-awakens-to-the-threat-of-sabotage-by-russian-agents.
3 “Poland says it breaks up Russian spy network”, Deutsche Welle, March 16, 2023, https://www.dw.com/en/poland-says-it-breaks-up-russian-spy-network/a-65004972.
4 Adam Easton, “Russian spy network accused of sabotage arrested in Poland”, BBC, March 15, 2023, https://www.bbc.com/news/world-europe-64971691
5 Chris King, “Mystery surrounds rescue of three Spanish divers near a strategic Baltic facility”, Euro Weekly, January 21, 2023, https://euroweeklynews.com/2023/01/21/mystery-surrounds-rescue-of-three-spanish-divers-near-a-strategic-baltic-facility/.
6 “Poland sets exclusion zone around Swinoujscie LNG terminal”, Reuters, April 12, 2023, https://www.reuters.com/business/energy/poland-sets-exclusion-zone-around-swinoujscie-lng-terminal-2023-04-12/.
7 Bartosz Sieniawski, “Secret Polish workshop repairs Ukrainian military equipment”, Euractiv, February 1, 2023, https://www.euractiv.com/section/politics/news/secret-polish-workshop-repairs-ukrainian-military-equipment/.
8 Szymon Zięba, „Zaskakujące ustalenia ws. hiszpańskich nurków. „Za szybko ich wypuszczono”", Trójmiasto.pl, January 17, 2023, https://www.trojmiasto.pl/wiadomosci/Zaskakujace-ustalenia-ws-hiszpanskich-nurkow-Za-szybko-ich-wypuszczono-n174566.html.
9 Sakshi Tiwari, “Chinese ‘Stealth’ Espionage! How Beijing-Backed Hackers ‘Acquired’ Sensitive US Tech Used In Its F-35 Fighter Jet?”, The Eurasian Times, February 3, 2022, https://eurasiantimes.com/chinese-stealth-espionage-us-tech-used-in-its-f-22-f-35-fighter/.
10 “Chinese hackers compromise’ US weapons systems designs”, BBC, May 28, 2013, https://www.bbc.com/news/world-us-canada-22692778.
11 Eric Auchard, “UPDATE 1-Israel’s Iron Dome’ makers were hit by hackers, expert says”, Reuters, July 30, 2014, https://www.reuters.com/article/israel-cybersecurity-missiles/update-1-israels-iron-dome-makers-were-hit-by-hackers-expert-says-idUSL6N0Q45LV20140729.
12 Ray Meiring, “How companies can prepare for the rise of cyberattacks amid the Ukrainian-Russian conflict”, Mission Critical, June 2, 2022, https://www.missioncriticalmagazine.com/articles/94128-how-companies-can-prepare-for-the-rise-of-cyberattacks-amid-the-ukrainian-russian-conflict.
13 Mateusz Chabros, „Cyberataki na Polskę przybrały na sile. Wśród atakujących prorosyjscy haktywiści”, Obserwator Gospodarczy, May 23, 2023, https://obserwatorgospodarczy.pl/2023/05/23/cyberataki-na-polske-przybraly-na-sile-wsrod-atakujacych-prorosyjscy-haktywisci/.
14 Alex Yankovski, “Key lessons from Ukraine’s eight-year struggle against russian cyber warfare”, KPMG, November 18, 2022, https://kpmg.com/ua/en/home/media/press-releases/2022/11/key-lessons-from-ukraines-eight-year-struggle-against-russian-cyber-warfare.html.
15 Google’s Threat Analysis Group, Fog of War How the Ukraine Conflict Transformed the Cyber Threat Landscape, p.
16 Ashish Dangwal, “Bayraktar TB2 Drones ‘Out Of Action’ From Ukraine War; Russia’s Air Defense Or Diplomacy Behind Their Disappearance?”, The Eurasian Times, December 4, 2022, https://eurasiantimes.com/bayraktar-tb2-drones-out-of-action-from-ukraine-war-russias/.
17 Daryna Antoniuk, “German arms manufacturer Rheinmetall confirms cyberattack”, The Record, April 14, 2023, https://therecord.media/rheinmetall-cyberattack-germany-arms-manufacturer.
18 Kevin Townsend, “Killnet Releases ‘Proof’ of Its Attack Against Lockheed Martin”, Security Week, August 12, 2022, https://www.securityweek.com/killnet-releases-proof-its-attack-against-lockheed-martin/.
19 Alex Yankovski, “Key lessons from Ukraine’s eight-year struggle against russian cyber warfare”, KPMG, November 18, 2022, https://kpmg.com/ua/en/home/media/press-releases/2022/11/key-lessons-from-ukraines-eight-year-struggle-against-russian-cyber-warfare.html.
20 Shields Up: Guidance for Organizations, Cybersecurity & Infrastructure Security Agency, accessed July 11, 2023, https://www.cisa.gov/shields-guidance-organizations.
21 Shields Up: Guidance for Organizations, Cybersecurity & Infrastructure Security Agency, accessed July 11, 2023, https://www.cisa.gov/shields-guidance-organizations
22 Alex Yankovski, op. cit.
23 Shields Up: Guidance for Corporate Leaders and CEOs, Cybersecurity & Infrastructure Security Agency, accessed July 11, 2023, https://www.cisa.gov/shields-guidance-corporate-leaders-and-ceos.
24 Ibidem

Conclusion

There are many similarities between the Ukrainian and Polish defence industries. For example, both dominant players are state-owned enterprises. Nevertheless, the permanent underfunding of these two industries over the past 30 years had revealed consequences. A situation that began to change only about a decade ago.

Despite such a situation, the cooperation between Poland and Ukraine in the arms industry sector has a bright future, and a number of factors contribute to it. One such factor is that both countries have a common strategic interest in the field of security and defence, a shared perception of security threats and challenges and a cultural proximity between the two countries that helps to strengthen bonds. They also share experience in terms of military industry cooperation. Not to mention, since being invaded by Russia, Ukraine has been testing new military equipment, and Poland (of all countries actively supporting Ukraine in Europe) played the most vital role. Throughout the war, Polish facilities have enabled the transmission of military supplies across borders, into war-torn Ukraine, but have also been a point of repairs for damaged Ukrainian military equipment. Such a highly-visible synergy of Ukrainian battlefield experience and Polish military technology is sure to bring a lot of benefits in the future.

There are also many other common areas in which the two nations could achieve good results (on a cooperative basis). Among these, the domain of land weapons, such as armoured vehicles, anti-aircraft and artillery systems, etc., can be pointed out first and foremost. Although, in some cases, the Polish military does indeed have a significant advantage in its military advancements (for example, in it's contemporary technology related to the maritime domain, unmanned systems, etc.) in others, Ukraine is more advanced (for example, in solutions to the production of transport aircraft). In any case, it is crucial to take advantage of emerging opportunities while also dealing with the challenges posed by current conditions.

Subsequently, the international community is in favour of extending cooperation with Ukraine and Ukrainian entities in the face of the outrages done by Russia. At this point in time, all sorts of deliberations, initiatives and active support towards Ukraine are anticipated to lead to an eventual involvement of Ukraine into the EU and NATO processes and programmes, including defence industrial assistance and joint Research and Technology (R&T) projects. With the constant growth of EU funding for defence Research and Development (R&D), there are new ways and opportunities to finance military-related projects. Polish entities may even become a leading example in engaging adequate cooperation among all of the countries in Europe actively sending aid.

Despite these high hopes, every cooperation in this highly sensitive field will need heightened security standards. Both Polish and Ukrainian sides, which engage in such a cooperation need to be aware that they become a target of Russian and Belarussian hostile activity both in the kinetic and cyber-security field. Therefore this awareness of the landscape of threats requires the incorporation of a security designed to meet all the requisites of mutual initiatives and joint-efforts. Security must be protected and implemented before the start of these projects rather than during it. The security tools to protect against sabotage and any other hostile action in modern society must be introduced and must now include increased safety personnel and monitoring apparatus. It is beneficial to also introduce the necessary protective measures in cyberspace, which includes the adoption of the best and well-known measures to increase cyber defence of the relevant establishments. Only a well-protected partnership between Ukrainian and Polish industries will enable the cooperation and a benefit for both sides.