The Copernicus Journal of Political Studies 2019
No. 1/2019, pp. 43–64
ISSN 2299-4335
DOI: http://dx.doi.org/10.12775/CJPS.2019.003
www.apcz.umk.pl/czasopisma/index.php/CJPS

Michał Piekarski
University of Wroclaw

POLISH ARMED FORCES AND HYBRID WAR: CURRENT AND REQUIRED CAPABILITIES

ABSTRACT

The article describes the problems of Polish military forces in the context of a relatively new type of threat, commonly described as "hybrid warfare". The first step of the analysis is a description of such threat, based on data gathered by Polish and foreign analytical centers. The next step is a presentation of the current state of Polish military forces – in terms of doctrine, organization, training and materiel (e.g. equipment). This kind of data analysis offers relevant information about defense capabilities that the Polish Armed Forces have and those which they lack. These capabilities are then compared to the challenges posed by hybrid warfare, thus providing insights on potential new capabilities which should be acquired as well as those which are unnecessary in the context of hybrid war.

Key words

Poland, military security, hybrid warfare, Baltic Sea

Introduction

"Hybrid warfare" has become a term often used in security research and international studies since 2014 and Russian-led actions towards Ukraine, notably during the Crimean Crisis and the conflict in Donbass industrial area. In the latter case, Russia managed only to create two puppet republics unrecognized by the international community, and the final result may be described as a draw – albeit one that was costly for the Ukrainians, particularly in the early stages of the war. However, the former action resulted in the annexation of Crimea and gave Russia full control of strategically important air and naval bases.

It must be noted that during those operations Russia was not using its armed forces in combat in an overt manner – a situation unlike traditional inter-state armed conflicts, where both sides openly use their troops. This time, Russia used a mix of elements – including non-state actors (ethnic minorities or criminal elements), funded or otherwise supported by intelligence services; units of special operations forces (SOF), called in Russia "Spetsnaz", which by their nature are used in a covert manner; "volunteers" or other personnel formally not connected to the Russian military (the infamous "polite green men") – supported by informational warfare (predominantly in the form of fake news) and shows of force, usually under the guise of various forms of military exercises. Those actions managed to exploit weak points in Ukraine's defense systems – not only in terms of terrain or equipment but most notably in the society as well as the military and law enforcement forces. A detailed analysis of this conflict can be found in numerous sources, for example a book by Bogusław Pacek (2018).

Emergence of this new type of threat raises a question about possible ways of countering hybrid warfare, above all from the perspective of Poland and the Polish Armed Forces. Thus an underlying thesis of this article is that this new threat requires from the Polish military a new set of military capabilities.

1. Hybrid warfare – definition and threat analysis

Mixed forms of force use is certainly not a new tool in international politics or military tactics. Propaganda and disinformation have been used in war since it emerged in human history. Actions like shows of force or other indirect

threats also have always been common. Covert use of military personnel, called "volunteers", "contractors", "advisors" or otherwise was also practiced, notably when one country wanted to avoid legal and political problems which would follow an open intervention. For example, in 1920, a division of the Polish army staged a "mutiny", therefore absolving the Polish government of responsibility for the capture of Vilnius and part of Lithuania. The short-lived Republic of Central Lithuania was later annexed by Poland, ostensibly in full compliance with the international law. Similar stories can be told about various Cold War-era colonial wars. For example, American covert operations in Southwest Asia were supported by a "civilian" airline called Air America, and in order to overthrow the Castro regime during the Bay of Pigs Invasion, a force consisting of Cuban exiles was formed by the CIA and supported by American warplanes flying without national markings.

Perception of hybrid warfare and security environment is different in the West and in Russia, which may lead to further problems with definitions and terminology (Wojnowski, 2015). However, the terms most commonly used are "hybrid warfare" or "hybrid threat". As the authors of a report published by the Danish Centre for Military Studies note, "The key aspect of hybrid threats is the deliberate 'blurring and blending' of types of adversary organizational forms (regular forces, irregular forces, terrorists, criminals), types of weaponry (from 'modern military capabilities' to improvised explosive devices (IEDs)), tactics ('traditional,' irregular, terror, and 'disruptive social behaviour,' including criminal), directed at different targets or foci (adversary military forces, civil governmental institutions, the civilian population, the international community, the international legal order, and domestic audiences of all parties)" (Murphy, Hoffman & Shaub, 2016, p. 3).

Therefore, a key aspect of hybrid warfare is not the employment of non-conventional tactics or techniques but the fact that they are used in a coordinated, deliberately mixed form. Another report, published by the West Point Military Academy, describes several forms of hybrid threat, putting them into a spectrum comprising two domains: "Gray Zone Hybrid Threats" and "Open Warfare Hybrid Threats". Gray zone threats are those where only covert means are used – information warfare, intelligence activities, or employment of non-state actors such as criminal networks. Kinetic and non-kinetic means are used as well (including demonstrations, political actions etc.). Open-warfare hybrid threats add another layer, which is open use of military power combined with unconventional means (Chambers, 2016, p. 22).

Such interpretation remains consistent with a major Russian doctrinal concept, called the "Gerasimov Doctrine". In this model of "new generation warfare", emphasis is put on shaping the environment, using non-military ways (e.g. political and economic), special operations, disinformation, deception, and internal destabilization of the attacked country, including bribing or intimidating officers and public servants to abandon their duties. Internal opposition is created by the arrival of pro-Russian militants, not acting openly but under the guise of contractors or another suitable cover – they may pose as activists, businesspeople or even criminals. It is also possible that they will not be soldiers or intelligence operatives but specially recruited and trained "volunteers", not necessarily recruited in Russia. However, they may be accompanied by special forces soldiers acting as commanders or "advisors". In this case, guerilla-like formations, such as armed militias or other armed irregular groups may appear; from the military perspective, in such a situation the operational environment will be "high-tech insurgency", blending guerilla tactics with advanced technical equipment and weapon systems, mostly lightweight ones (such as firearms, machine guns, mortars and portable missile launchers) which can be covertly smuggled into the target country.

Preparing for such operations may begin long before the conflict. This includes establishing and maintaining safehouses and other facilities suited for hiding people and equipment. In this context, an interesting situation occurred in 2018 in Finland, where the police and the border guard raided two small islands where a number of multi-bedroom houses were built, along with nine boat piers and a helipad, raising suspicion that those facilities – owned by a Russian businessman – had been prepared for use by Russian special forces in case of a crisis (Higgins, 2018). Subsequent preparatory phases consist of operations like blockades or enforcing "no-fly zones" which make attacked country more vulnerable and cut off from external support.

Finally, military operations commence. Nowadays, the Russian doctrine emphasizes using modern, precise strike weapons, including long range artillery, guided missiles and electronic warfare. The use of conventional military forces is thus limited and can occur only in highly permissive environment. It is evident that such a model makes it possible to reduce the duration of the conflict, helps avoid an intervention of the attacked state's allies and reduces losses in Russian military forces (Berzins, 2014). Most likely, only the air force, missiles and artillery are used instead of typical land operations. A short strike aimed at key infrastructure of the attacked state (e.g. power plants) may help achieve political

goals without the need to face obvious political and military consequences of occupation (even a temporary one).

Considering this, hybrid warfare may even replace conventional warfare as a tool of Russian policy as it is a more cost-effective solution. It should be therefore assumed that this type of threat is a scenario that is equally or even more dangerous and likely to occur in Central and Eastern Europe than a conventional armed conflict.

Certainly, the use of hybrid methods, especially from the domain of gray-zone hybrid threats, requires certain conditions to be met – most notably because great emphasis is put on disinformation, destabilization, and other ways to weaken the target country and society from the inside. The attacker must detect and analyze divisions and grievances in the society in order to exploit them. Such openings may include social (class) divisions as well as ethnic, religious or language issues. Other cultural or economic issues may also become relevant.

Due to their nature, such issues should be considered as highly politicized problems. Only then can they be recognized as significant. This is especially important with regard to blocking external support for the attacked country. Nowadays it is almost impossible to block such support for a country attacked by terrorists; however, if there is an opportunity e.g. to portray its government as violating rights of ethnic minorities, the political will of its allies may be weakened. An easy way to achieve this goal can be a simple provocation during a peaceful demonstration, which would convince the police forces to use heavy-handed tactics and, as a result of an informational campaign, generate a negative image of the attacked country. There are numerous options, but they all must be tailored to the current situation within a given country, to its society, economy and culture and – most importantly – to the intent of the aggressor.

2. Hybrid warfare – a challenge for Polish national security

In the case of Poland and its neighbors, the most likely scenario of a hybrid conflict assumes Russia's desire to rebuild its old sphere of influence, predominantly by retaking the control over the Baltic republics (Lithuania, Latvia and Estonia), thus linking the Kaliningrad District back to the Russian mainland via a land connection and regaining wider access to the Baltic. It is not only a matter of national pride; like in the case of Crimea, the main issue is location of military forces and installations. Because Poland and the Baltic States are members of NATO, this means that Western forces may be (and in fact, are) deployed close

to Russian cities – notably, Sankt-Petersburg. According to General Pacek, this problem has been noticed by the Russian expert N. Komleva, who claims that the border areas between Russian and Western civilization (called "limitrophe states") shall be theaters of hybrid wars, and the conflict in Ukraine is example of such a war (Pacek, 2018, p. 15).

From the political point of view, regaining control over those three republics may seem an easy victory for Russia. A successful operation of regime change in member states of NATO and the UE, conducted in a manner which would prevent those organizations from responding effectively, would certainly humiliate them and prove them ineffective. Yet such victory would also have important consequences in Russia's domestic politics, demonstrating to the population that the country is powerful and the government can be trusted, especially in times of crisis. Such a scenario would be similar to the Falkland War, when the Argentine junta tried to win back public support by seizing the islands in hope that the United Kingdom would not be able to counterattack. Russia can hold similar hopes regarding the small – and easy to conquer – Baltic states. It is easy to imagine that after escalating ethnic conflicts in the Baltic states, which have large Russian-speaking minorities, Russia could mount a fast military operation aimed at seizing those republics (likely under the guise of a "humanitarian intervention") in a manner preventing NATO from effective response. Scenarios in which a number of hybrid means, both overt and covert, would have to be used to delay or stop the allied response, and the Russians would be able to reach the outskirts of Latvian and Estonian capitals in about sixty hours were wargamed by RAND Corporation in 2016 (Shlapak & Johnson, 2016).

In such a scenario, Poland plays an important role as the only NATO country with a land border with Lithuania, known as the Suwalki Gap. Polish ports, air bases, roads and railroads are crucial in providing assistance to the Baltic states. Poland also has aspirations to be one of the key players in this part of Europe, primarily as a close ally of the United States. The Baltic region is considered as particularly vulnerable. If movement of NATO forces through the Suwalki corridor was denied, Russia could gain a significant strategic advantage in the Baltics. NATO forces would have to mount a counteroffensive to regain this area, and during that time the Baltic states could be seized or forced to surrender. The importance of the Suwalki Gap has been already described in several documents, including reports by US-based think-tanks (Fabian, Gunzinger, van Tol, Cohn & Evans, 2019; Hodges, Bugajski & Doran, 2018). From the Russian perspective, American military presence in Poland – especially that of air force units, special

forces, intelligence gathering systems and a ballistic missile defense base – may be considered as serious threat.

Finally, Polish long-term foreign policy does not agree with that followed by Russia as Poland has generally supported pro-democratic and anti-Russian tendencies in the Baltic states, Ukraine, Belarus and even Georgia. Therefore it is clear that Poland may be a victim of hybrid warfare. In the most likely scenario, the goals of such an operation would be as follows:

1) to prevent the use of Polish and allied armed forces and infrastructure (roads, railroads, ports, airfields, staging areas) in assistance to Lithuania, Latvia and Estonia;
2) to force Poland to withdraw from any activities which would be contrary to Russian interests;
3) possibly to force Poland to allow Russia to establish a land connection to the Kaliningrad District or at least to cut Polish land connection to Lithuania;
4) possibly to force Poland to remove American and other NATO forces from the Polish territory.

Such strategic goals mean that possible hybrid warfare against Poland would be an operation aimed at shaping domestic and international public opinion, as well as influencing policy-makers – by using information, disinformation, sabotage and other methods, including overt military means – that the cost of Polish participation would be much higher that any gains.

However, unlike Ukraine and the Baltic states, Poland does not have large ethnic or language minorities, so escalation of ethnic or language conflicts is difficult and unlikely, so other weak points need to be found. It is also difficult to find any relevant political or social movements which would have any credibility and could be overtly used by Russia. That leaves only false-flag scenarios in which any attacks would be conducted in a manner suggesting that someone other than Russia or a Russia-controlled actor (a state, a group, an individual) is responsible. Such operations could be meant to exacerbate other existing divisions and conflicts, which in Poland have mostly cultural and economic background and take the form of a division between the western, mostly urbanized and liberal part of the country and the eastern, more rural and conservative part. In recent years, those divisions have been visible not only in election results but also in attitudes towards the role of the Catholic Church in the society and LGBT rights, perception of modern history etc. It is easy to imagine a provocation, for example a bombing during a Catholic mass in a highly symbolic place such as a cathedral or monastery, followed by a fake message claiming that a left-wing

organization is the culprit – or an attack on an equivalent symbolic target like Gay Pride March, liberal politicians or journalists, where a right-wing group would claim responsibility. Such operations could lead to escalation of conflicts in the society, and possible further attacks. In such situation, the government would have to focus on quelling the internal violence, instead of supporting allies. A drawback of such an option is the amount of time required to prepare and conduct this type of operation. It is also unclear how effective fake messaging would be – how many people would believe and follow them and how opinion leaders in Poland would react (Piekarski, 2019).

Another possibility would be an attack on material resources. This option is easier because it does not involve elaborate manipulation of public opinion; it requires only identifying key elements of infrastructure and striking at them. This might involve for example an attack on military installations, such as airbases which are needed to support the Baltic States, or on logistic bases, where fuel, spare parts and munitions are stored. The downside is the fact that military installations, especially those used by NATO forces, are better protected and less vulnerable to sabotage than civilian installations. It is possible to attack them, for example with drones, light mortars or portable rocket launchers to reach airplanes on aprons, but the use of such advanced weapons is a clear trademark of an operation conducted by special forces, not domestic terrorists. Also, it is not easy to predict the reaction of Western governments and public opinion if NATO service members were killed.

Attacking civilian targets, especially those classified as critical infrastructure, is easier and does not involve the problems discussed above; it offers a chance to represent such crisis as a Polish-only problem, or even to blame Poland for the outcome.

Such targets are likely to include:

- energy-related infrastructure: power plants, electrical substations and transmission lines, oil refineries, petroleum storage sites and pipelines, and liquid natural gas terminals, pipelines and storage sites;
- transportation infrastructure, particularly its elements used also for military purposes, such as airports, railroads and railroad yards;
- communications systems.

A possible scenario could be a blackmail-type attack. In case of an international crisis, Russia could use its special operations forces to attack critical infrastructure. Of course, such attacks would be still false-flag attacks, but a media campaign would be secondary to political pressure. It is quite possible

that the factor of information warfare will be less and less important when increasingly hard measures are used.

As in the case of every modern state, Polish economy depends on energy resources and effective transportation and communications. A serious disruption in those spheres during peacetime would bring the economy to the brink of the crash – factories not receiving components and unable to ship out assembled products, logistic centers becoming chokepoints, and most of public services ceasing to function due to lack of fuel and power. Any serious international crisis would only multiply the effects. It is therefore possible that such punitive measures would be aimed at forcing the Polish government to change its policy and withdraw from supporting its allies.

However, there are other options as well. Because Poland imports Russian coal, natural gas and oil, it is vulnerable to an embargo. This vulnerability may be limited by diversification because those energy sources may be imported from other countries – especially by the sea. Yet this option may be in turn blocked by a covert sabotage operation, i.e. a "terrorist" attack on a liquid natural gas or oil tanker, resulting in an environmental disaster and possibly a degree of damage to port installations. A highly likely course of action would be covert placing of mines, including custom-made explosive devices, in the sea or in port waters. This could be done in a covert manner, with submarines or even civilian vessels used as platforms for unmanned underwater vehicles or divers. Mines could be placed in advance; they could also be programmed to detonate only if a signature (likely acoustic) of a specific ship was detected, assuring that only tankers or military sealift vessels were attacked. That would provide high political gains and certainly would be used in propaganda activities, followed by Russian maritime blockade and a "maritime security operation" allowing Russia to dominate the Baltic under the guise of protecting international shipping lines and the natural environment (Matuszewski, 2016). It is quite possible that during such an operation Russia would use various elements of kinetic and non-kinetic action. Apart from just deploying ships, a very likely element would be harassment of Polish ships and commercial vessels by e.g. low-level flights of naval aircrafts, turning on targeting devices (radars), aiming guns, and jamming radio communication and navigational systems (especially GPS). It is also possible that Russian ships would enter Polish territorial waters as a *fait accompli*, demonstrating Poland's failure to protect its borders. If challenged, Russian forces might conduct kinetic operations and destroy ships or land targets, claiming that it was a response to a Polish attack. Again, such operation would be heavily supported by propaganda activities.

Thus threat at sea requires serious consideration. Even sheer threat of maritime blockade or another similar crisis may force shipping companies to stop their activity in the Baltic area due to threat to ships and crews; this in turn would disrupt industrial cooperation networks. Economic losses might then force the government to make certain political decisions. Long-term effects could be even withdrawal of international corporations from Poland, which might be perceived then as too insecure a place for manufacturing and services.

It also may be possible that Russia would use other forms of disrupting transportation in Poland, particularly during a crisis, when columns or military vehicles and railroad convoys would be moving to the Baltic states and to eastern Poland. Then, special operations forces of Spetsnaz-trained groups might be used to ambush road convoys and disrupt railroad traffic.

Another stage of a hybrid war is use of overt military measures, within a fully or at least partially shaped environment; the use of such measures would be likely limited in time. In this context, another element of Russian capabilities are missile systems, including the well-known Iskander systems and Kalibr cruise missiles used to attack land targets; surface-to-air missiles (SAMs) S-300, S-350 and S-400 in a range of variants; and anti-ship systems Bal and Bastion. Those long-range systems may be used to create zones in which any land, air or naval operations are difficult. Consequently, these systems are nowadays called "Anti-Access/Area Denial" (A2/AD). Such an "umbrella" or a "bubble" would create permissive environment for Russia to use air, naval and land forces. However, an important problem is the real capability of such systems, in particular their target detection range (which varies depending on terrain features, distance, target size, or flight altitude in case of air threats). Another option may be to use missiles and other precision-guided weapons to strike at elements of critical infrastructure, which are easier to target (firstly because they are stationary), the number of direct casualties is limited, and destruction of power plants, refineries or similar facilities may have drastic consequences for the attacked country (Dalsjo, Berglund & Jonsson, 2019)

It is thus clear that hybrid threat may appear in different forms. In its early stages it may be mistaken for legitimate political or media activity (including social media activism). Later, special operations forces may be deployed – but this again can appear to be legal activity or remain unnoticed. For example, teams of special forces may use the High-Altitude High Opening technique, jumping from aircraft long before flying over the state border and landing after a long gliding descent (up to 40 kilometers). The plane may be detected and tracked but is likely to be considered a civilian or training flight. Another option may be

covert deployment of divers and their equipment from a submarine or a research vessel.

The above analysis presents an interesting mix of adversary courses of action, tactics and tools. On the high end of this spectrum there is a threat of precise missile strikes. On the low end, there are riots, sabotage actions, assassinations or other terrorist-type attacks, including special forces raids using explosive devices, small arms and other light weapons (light mortars, RPG-type launchers etc.). There is very narrow space for middle-ground approach, which would be a conventional, large-scale land invasion supported from air and sea. Also, it is clear that various forms of electromagnetic warfare and cyberwarfare will be used. They may involve jamming radio communication and GPS signals, spreading malware in computer networks, as well as various forms of intelligence gathering activities.

3. Polish Armed Forces: current organization and capabilities

At present, the Polish Armed Forces are composed of five major services: the Land Forces, the Navy, the Air Forces, the Special Operations Forces and the recently created Territorial Defense Forces. Two supporting services are the Military Police, which is responsible mostly for law enforcement in the military, and the Armed Forces Support Inspectorate, which handles logistic support tasks. The Land Forces, the Navy, and the Air Force do not have separate commands. Only the Special Operations Forces have a command element, but subordinated to the Armed Forces General Command. This command is responsible for managing their personnel resources, training and equipping subordinate units in peacetime, and acting as a "force-provider". The role of a "force user", a commanding organ in case of crisis or war is delegated to the Armed Forces Operational Command, again with the exception of the Special Operations Forces. The Territorial Defense Forces have their own command, equal in status to the two commands mentioned above. Finally, the General Staff of the Polish Armed Forces is responsible for long-term planning. The command structure is supported by the Warsaw Garrison Command, which provides support and security for highest-level commands and maintains command and communications units for use in case of crisis or war.

The Land Forces are currently composed of three fully-fledged divisions (two mechanized and one armored) with the fourth (also mechanized) being formed at the moment. There is also a number of separate brigades and regiments,

notably airborne, airmobile, engineer, reconnaissance, air defense and other specialized units. The Navy comprises two flotillas, which are composed of ship squadrons and shore units. There is also a brigade of naval aviation and other support units. The Air Force has four aviation wings (two tactical, one transportation, one training), one air defense missile brigade and one radio-technical (Radar) brigade. The Land Forces, the Navy and the Air Force also have separate signals intelligence components. The Military Police is divided into regional components (units and detachments) and has two mobile units, one being a counterterrorism-trained unit, while the second is trained as a mobile military police unit. The Territorial Defense Forces are planned to be composed of brigades and battalions, matching the administrative division of the country (a brigade in each voivodeship, plus an additional brigade in Masovia). Finally, the smallest of services is the Special Operations Forces, composed of five units with different roles, including a dedicated counterterrorist unit GROM, the Commando Military Unit (able to conduct special reconnaissance and direct actions such as raids), the Formoza Military Unit (a maritime counterpart of the Commando Military Unit) and the support units Agat (kinetic support and direct actions) and NIL (communication, medical, intelligence and logistic support) (Tymoczko & Banaś, 2019).

The Land Forces have a large number of tanks: 247 German-made Leopards 2A4/A5 and 690 units of the T-72 family, Soviet-designed and produced in Poland (including 232 units of Polish-upgraded variant PT-91). The number of infantry fighting vehicles is even larger: 1277 tracked BWP-1 and 359 much more modern wheeled Rosomaks. Also 282 light scout BRDM-2 vehicles are used (some after local upgrades). As to other land systems, the artillery is well equipped in terms of quantity: 546 howitzers and mortars of caliber larger than 100mm and 180 rocket artillery launchers – all 122mm caliber. However, most of those systems had been acquired before 1990, only a small number of self-propelled Krab howitzers and self-propelled Rak mortars have been delivered recently. Besides, after 2003, 264 Spike-LR infantry anti-tank guided missiles have been purchased (Dmitriuk, 2018). Additionally, in 2019 Poland signed a contract to purchase one battalion of the American HIMARS long-range rocket system.

The land forces are therefore reasonably equipped to conduct conventional, large-scale operations, with secondary options of using mechanized forces in different capabilities, which applies mostly to Rosomak-equipped battalions. Also, light forces – the 6th Airborne Brigade, the 25th Air Cavalry Brigade, the 21st Podhale Rifles (Mountain) Brigade as well as engineer and reconnaissance regiments can be used in a variety of crisis response situations. Notably, air mobility

capability may contribute to flexible response; however, the limited capabilities of helicopter units can be a hindrance in this aspect.

The majority of helicopters in Land Forces units, including all attack Mi-24, had been manufactured before 1989; only 32 W-3 Sokół-type crafts and several Mi-17 utility helicopters are younger. Apart from utility and cargo helicopters, Mi-24 do not have currently any anti-tank capability due to lack of available guided missiles, and there is no clear information as to their possible replacement. Some of Sokół helicopters have been upgraded to a combat search-and-rescue Głuszec model (one squadron, dedicated to personnel recovery missions) and signals intelligence Procjon version. One unit was also converted to a battlefield surveillance / imagery intelligence version.

A similar situation can be found in naval aviation, where the most modern units are search-and-rescue Anakonda (a version of Sokół) helicopters and light patrol Bryza airplanes, which are used for maritime patrol and surveillance duties. They may provide targeting data for other components of the Navy with their Łeba (automated command and control system) terminals. A contract for four new helicopters, heavy AW101s, has been signed recently, but it is unclear how those helicopters shall be equipped and thus whether they will be used as maritime patrol/antisubmarine warfare or for search-and-rescue duties. With regard to combat and crisis-response capabilities, the Air Force are in the most comfortable situation, with a number of upgraded Sokół search-and-rescue helicopters and Mi-17 special operations-support helicopters (Dmitriuk, 2018).

Apart from helicopters, the Air Force has capabilities of significant quality for air operations – including counter-air operations, close air support, air interdiction as well as air surveillance – due to the 48 F-16C/D block 52+ multirole combat aircrafts, which may use a variety of precision-guided weapons. However, the number of aircraft is small, and other combat aircrafts – Su-22 and MiG-29 – have obsolete sensors and weapons, and no multirole capability; besides, after a series of accidents, at the moment of writing this article the MiGs are not used in active service (they have been grounded). Therefore, the potential of the Air Force is now almost entirely reduced to F-16s. This situation may change with the purchase of newer F-35 stealth aircraft, but the number of these expensive fighters will be limited (the plans are to buy 32).

Polish air assets also include unmanned systems. The Air Force, the Land Forces, the Territorial Defense Forces and the Special Forces operate a number of UAVs, including aircraft delivered from the United States and Israel as well as Polish-designed and manufactured light drones – FlyEye (surveillance and

reconnaissance) and Warmate (which may be used as loitering ammunition systems, capable of precision strikes against detected targets).

Air defense units – in the Air Force, the Land Forces and the Navy – have been less lucky, as most of their missile systems (codenamed "Newa" "Osa" and "Kub") are obsolete and have limited capabilities, particularly when Russian missile systems like Iskander or Kalibr are considered. The most modern components are light, short-range, man-portable or vehicle-mounted Grom missiles. Plans for a significant upgrade resulted only in the contract for two batteries of American-made Patriot PAC-3 missiles. In contrast, radar units are well-equipped with stationary long-range radars forming the Backbone network and with mobile systems working as a part of NATO Integrated Air Defense System. This element is also supported by signals intelligence systems (Dmitriuk, 2018).

Finally, the Navy uses a number of ships, including two guided-missile frigates (American O.H. Perry class), one corvette, four submarines, three missile boats, three minehunters, seventeen small minesweepers, one mine-countermeasure command ship, five minelayer-landing ships, two signals intelligence ships, and a number of training and auxiliary vessels. A part of those units require replacement due to age (some have been in service for over forty years), limited capabilities of sensors and equipment or other factors. An additional problem is that some of the ships were purchased second-hand, as temporary stopgap measures, yet plans to replace them with new vessels have not gone beyond the concept phase. However, in some sectors progress has been made. Missile boats are equipped with long-range RBS-15 Mk3 missiles, mine-countermeasure assets have been upgraded, and a new minehunter (ORP Kormoran) has been in service since 2017 and two more ships of this class have been contracted. An important asset is the Maritime Missile Unit, which is a land-based, mobile formation with two squadrons of long-range NSM missiles. This force – highly resilient and able to receive targeting data from a number of air, naval and land-based sources thanks to the national systems such as the Łeba automated command and control system as well as NATO C4I system – may act as Polish national A2/AD force in the southern Baltic area, covering also Russian ports in the Kaliningrad District.

However, the basic organizational scheme or sheer numbers do not provide actual information about the real potential of the Armed Forces to counteract hybrid threats. The most important element of assessment are the capabilities of the forces, which are nowadays strongly linked to weapons systems, sensors, and other pieces of equipment, as well as the ability to use the said equipment. It is clear that Polish Armed Forces have limited capabilities regarding the possible scenarios of a hybrid war. The quality and quantity of equipment and the fact

that most of manpower and budget are allocated to Land Forces makes them capable mostly to counter a conventional, large-scale land invasion, apart from airmobile units which are much more versatile. Anti-air capabilities – including the ability to engage cruise missiles – are highly limited, and there is no anti-ballistic missile capability (e.g. against Iskander missiles). Air-to-surface options are limited to F-16 armament, which includes a variety of missiles and guided bombs but, as stated above, the number of these airplanes is limited. Finally, regarding the age and equipment of its ships and aircraft, the Navy must be currently considered mostly as mine-countermeasures force and limited long-distance strike component.

In contrast, the Special Operations Forces and Territorial Defense Forces do have some important capabilities. They may be used in particular to detect and eliminate enemy special operations forces and protect critical infrastructure. Special Operations Forces are also able to conduct low-visibility and precise operations, and those capabilities may be crucial in case of a crisis. Their counterterrorist capabilities are especially important. Under current regulations, particularly the Act on Crisis Management, the Act on the Police, the Act on the Border Guard and the Act on Anti-terrorist Activities, the military forces are allowed to support police, the Border Guard and civilian crisis management administration, even in peacetime, especially if a terrorist accident has occurred or may occur, which provides increased flexibility in using military resources.

4. Desired capabilities and organization of the Armed Forces against hybrid threats

Due to the nature of hybrid threat, it is clear that tanks or self-propelled howitzers are an unlikely choice to counter sabotage, disinformation and other gray zone activities. Therefore development of the majority of such armed forces is outside the spectrum of this paper. One exception is artillery, including various types of guided missiles, due to their ability to carry out precision strikes. However, there are numerous other capabilities which may be useful.

Because hybrid threats may be difficult to detect, a crucial set of capabilities is Intelligence, Surveillance, Reconnaissance and Target Acquisition (ISTAR). While on daily basis a significant amount of information is gathered by law enforcement services, notably the Border Guard and the police, such data are mostly produced from routine document and vehicle inspections, interrogations, searches and confidential human intelligence sources, i.e. standard police work.

Only the Border Guard conducts surveillance of the border line and adjacent areas with the use of technical devices (including airplanes, helicopters, radars and low-light cameras).

However, certain elements of land forces may be used to augment law enforcement services. A special attention in this context should be paid to reconnaissance regiments. The Land Forces currently have three such units, which are able to conduct intelligence-gathering operations (e.g. patrols) or to cover observation posts in the border zone and in the areas where the risk of enemy activity is significant (i.e. around potential targets). That would allow allocating more law enforcement officers to other tasks. Apart from its tactical value, this capability offers also a significant political advantage: because soldiers would be used only as reconnaissance force that merely passes information to the police and the Border Guard, they would not make arrests or do searches, which could limit the political consequences of using military force in such roles.

ISTAR support for law enforcement services may be provided also by other components, which have resources the police lack. One of such resources are unmanned platforms, used by the Land Forces, the Air Forces and the Special Forces. Apart from quantity, in which aspect the Armed Forces have advantage, military systems like the FlyEye or Orbiter drones are less prone to jamming and other forms of interference.

Due to the legal status of open sea and its geographical conditions, the Baltic Sea is permissive environment for operating air and naval intelligence-gathering platforms. Especially ships are convenient to use because they may remain at sea for days and weeks, while manned and unmanned aircraft have duration times counted in hours but allow faster response. Therefore air and naval platforms complement each other.

Upgrading ISTAR capabilities is a major task within the framework of improving capabilities of the Polish Armed Forces. Currently, the Polish Navy uses two signals intelligence ships, the ORP Nawigator and the ORP Hydrograf, which were launched in 1975 and 1976 respectively (Ciślak, 1995). Being almost forty-five years old, they require replacement. New ships should allow gathering a variety of data and may also act as operation bases for underwater and airborne unmanned platforms.

Regarding airborne platforms, one of the priorities should be acquisition of early-warning aircrafts, the so-called "flying radars". Currently, the Polish Air Force does not have such equipment, and there were no plans to purchase it even though the ability to put airspace surveillance radar high above the ground level would allow faster detection of cruise missiles and planes carrying them.

However, recent plans regarding the purchase of F-35 fighters may offer a similar capability, regarding the vast potential of F-35 not only as a combat aircraft but also as a sensor platform.

Further gaps in defense are signals intelligence aircraft and maritime patrol planes; however, these two types were included in the Armed Forces Development Programs – but no contracts for those programs (codenamed "Płomykówka" and "Rybitwa") have been signed yet. Other extensive plans of purchasing a variety of unmanned platforms – dubbed "Zefir", "Orlik" "Gryf" and "Albatros" – were finalized only partially with a contract for forty short-range drones (the "Orlik" program). Other programs are to be finalized after 2021 or their status is unclear according to Tomasz Dmitruk, military journalist monitoring progress of technical developments of Armed Forces (Dmitriuk, 2019). Signals intelligence aircraft, maritime patrol planes and unmanned aircrafts are highly desirable and awaited development because capabilities in the area of signals and imagery intelligence facilitate surveillance of border and maritime areas, as well as offer support in protection of critical infrastructure and other activities.

Another element highly important in the context of hybrid threat are naval forces. The Navy may play a critical role in the mentioned scenarios that assume hostile activities would target ports and sea lines of communication. This requires a wide set of capabilities, notably in the areas of situational awareness and mine-countermeasure operations. Also, anti-submarine warfare, anti-surface warfare (capability to engage surface vessels), air defense and special operations support are needed here. Currently, three modern minehunters (of Kormoran II class) are contracted, and three more are expected. This shall bring a new quality to protection of Poland's maritime areas and shipping lanes against mine warfare, including hybrid-warfare scenarios (Dąbrowski, 2019). However, along with signals intelligence ships, such vessels need protection, especially from air threats and land-based or ship-based missiles. Mine-countermeasure vessels are also incapable of conducting other operations, particularly in anti-surface warfare and air defense domains. The latter tasks require multipurpose surface combat ships in form of guided-missile frigates or large corvettes, capable of area air defense, armed with long-range surface-to-air missiles. A 2018 attempt to acquire such ships (Australian Adelaide-class frigates) failed. However, given the capabilities of modern guided-missile frigates, it is necessary to purchase at least two such ships. Their presence may not only limit Russian options regarding air and missile strikes but also supplement Polish A2/AD capabilities, complementing the Maritime Missile Unit (Ogrodniczuk, 2018). Owing to their ability to detect, deter and deny any adverse actions, frigates may provide

situational awareness (notably by radar and sonar systems) and offer reliable protection to commercial shipping and military sealift efforts in hybrid warfare scenarios. The very presence of well-armed warships may produce significant political results and would make it possible to prevent or respond in kind in previously described scenarios of naval hybrid warfare. Also, those ships can act as platforms for manned or unmanned helicopters and unmanned surface and underwater vessels, allowing better situational awareness. Therefore, acquisition of two to four multipurpose surface combatants would provide a necessary set of capabilities for the Navy.

Another capability which requires upgrade is the ability to rapidly respond and move troops and equipment in crisis situations. Light airmobile forces already exist and can be highly efficient as quick response forces. In case of hybrid warfare, an important element of operational environment is that the threat of conventional heavy weapons is limited as the enemy most likely would consist of guerilla-like forces. This creates permissive environment to use light forces, able to counter threat from light weapons systems, especially portable air defense weapons (like Russian Igla or Striela). Given the current quantity and quality of military helicopter fleet, it is necessary to acquire a number of medium-sized, multirole helicopters as replacement for the Mi-8/Mi-17 family. Such replacement should allow quick deployment of elements of special airborne and airmobile forces in a crisis area, and thus provide an airframe of troop-carrying capability similar to or exceeding the Mi-8 family – which means 20 fully equipped soldiers or even more per craft. Such helicopters need to be protected from enemy weapons by countermeasures (detection and warning devices, flare dispenser) and must be armed with machine guns or similar weapons for self-defense purposes.

These conditions shed some light on requirements for combat helicopters, which would also operate in such environment of limited threats. Therefore an important question arises about a Mi-24 replacement, which may be a typical, expensive attack helicopter or merely an armed utility helicopter which is, however, capable of carrying precision-guided ordnance. Given modern capabilities of guided missiles, a helicopter may stay in safe distance from the target – even more than ten kilometers away, so using an armed multipurpose helicopter instead of a typical attack one seems a viable option.

There is also another role for helicopters as naval forces need dedicated combat and search-and-rescue variants. Dedicated airframes are required as support for special operations forces and personnel recovery missions. As far as hybrid warfare is considered, it is possible that one platform – a multipurpose

medium-sized helicopter in several variants – from troop-carrying to special operations support – could fulfill all those requirements.

To speak further about air forces, an issue that must be addressed is A2/AD systems. In case of overt use of force, the role of air defense will be the key to survive attacks, and it is crucial to have sea- and land-based long-range air defense systems, able to counter ballistic and cruise missile threat. This necessitates deployment of modern systems, which would primarily mean more "Wisła" (MIM-104 Patriot) batteries and – in a supplementary role – shorter range missiles, which are planned to be purchased in the "Narew" program. Given the growing role of guided missiles, the role of fighter planes should be carefully analyzed. Clearly it does not mean that fighters will be replaced by missiles, but it is quite possible that airplanes shall act more as sensor platforms and nodes of air defense systems datalinks, connecting ground- and sea-based platforms, unmanned aircrafts and other assets, which may limit the number of required manned aircrafts. This invites another question about the role of a new generation of fighters, such as F-35 (Kamizela, 2019).

Another sphere of great concern includes communication, command and control, and cyber capabilities. As it was mentioned earlier, various forms of warfare in electromagnetic spectrum and in cyberspace are very likely to be used. In Polish Armed Forces this problem is exacerbated by the fact that a large number of communications devices are obsolete, and vulnerable to jamming and transmission interception. Introduction of a new communications system must be considered a priority, especially in the Land Forces.

Two elements of the Armed Forces which have capabilities allowing them to counter hybrid threats are the Special Forcers and the Territorial Defense Forces. Regarding the latter, any serious fact-based assessment will be possible after the current process of forming brigades and battalions ends. However, such forces may be particularly important as security elements guarding critical infrastructure, including roads and railroads. This aspect should be considered as the most important mission of these forces, which ought to be reflected in their organization, training and equipment.

Special Forces may be particularly useful it two roles. One is covert intelligence gathering (special reconnaissance), which may be conducted in a variety of environments. In this role, they can support counterintelligence services and the police. The other are direct actions against enemy forces, in particular the leaders or key elements of enemy forces – and in this capability they could support police counterterrorist units. Such cooperation at the tactical level is already well developed, though mostly in the form of joint training exercises,

so it can be predicted with a fair amount of certainty that in case of a real joint operation, military and police forces will be able to cooperate effectively. From political perspective, special forces are able to operate in low-visibility manner.

A similar level of cooperation is required when other elements of the national security apparatus are considered. This applies to emergency and rescue services, i.e. the Emergency Medical Services and the National Fire Service but also to the Civil Defense. The last service in particular has currently very limited resources. It must be assumed that if mass-casualty incidents occur as a result of hybrid warfare (i.e. extensive damage to critical infrastructure), military aid will be required. This means that those capabilities which are not strictly combat-related – like medical, search and rescue, engineer or logistic units – may be as important in countering hybrid threats as combat components.

Summary

Due to the nature of hybrid threats, particularly those of the gray zone spectrum, which may appear in various form, including terrorist attacks, riots or organized criminal activities, a wide set of capabilities is needed to face them. The problem of countering hybrid threat is not limited to desired capabilities of the Polish Armed Forces in domain of traditional combat units. It also encompasses those which may seem to have lesser importance, like support elements. Tanks, tracked infantry fighting vehicles, and short-range air defense systems have a role to play in conventional conflicts, but in hybrid warfare scenario, where open warfare hybrid threats are only one element of the spectrum, their role is limited. Therefore those types of equipment, as well as heavy-tank and mechanized forces in general, should not be treated as a priority in defense policies, especially with regard to budget expenditures. More important elements of the Armed Forces, especially in the context of gray zone hybrid threats, are quick reaction forces (airmobile units), special forces and territorial defense units. In certain situations, naval forces may play a significant role as well. In the light of the above, Poland should regard hybrid warfare as one of main challenges for its armed forces, focusing the national security policy and defense planning on maintaining and developing capabilities relevant in countering hybrid threat.

REFERENCES

Berzins, J. (2014, Apr). Russia's New Generation Warfare in Ukraine: Implications for Latvian Defence Policy. *Policy Paper*, *2*. Riga: National Defence Academy of Latvia, Center for Security and Strategic Research.

Chambers, J. (2016). *Countering Gray Zone and Hybrid Threats*. West Point: Modern War Institute, United States Military Academy.

Ciślak, J. (1995). *Polska Marynarka Wojenna*. Warszawa: Lampart.

Dalsjö, R., Berglund, C., & Jonsson, M. (2019). *Bursting the Bubble: Russian A2/AD in the Baltic Sea Region: Capabilities, Countermeasures, and Implications*. Grindsjön: Swedish Defence Research Agency.

Dąbrowski, K. (2019). Hugin 1000 MR. *Frag Out! Magazine*, *24*, 30–37.

Dmitriuk, T. (2019). Stan realizacji Planu Modernizacji Technicznej (systematyczna aktualizacja). Retrieved from http://dziennikzbrojny.pl/artykuly/art,2,4,10344,armie-swiata,wojsko-polskie,stan-realizacji-planu-modernizacji-technicznej-systematyczna-aktualizacja

Dmitriuk, T. (2018). Dwie dekady w NATO – modernizacja techniczna Sił Zbrojnych. *Nowa Technika Wojskowa*, *8*, 16–29; 9, 6–15; 11, 8–17.

Fabian, B., Gunzinger, M., van Tol, J., Cohn, J., & Evans, G. (2019) *Strengthening The Defence Of Nato's Eastern Frontier*. Washington: Center for Strategic and Budgetary Assessments.

Higgins, A. (2018). On a Tiny Finnish Island, a Helipad, 9 Piers – and the Russian Military? Retrieved from: https://www.nytimes.com/2018/10/31/world/europe/sakkiluoto-finland-russian-military.html

Hodges, B., Bugajski, J., & Doran, P. (2018, Jul). *Securing the Suwałki Corridor: Strategy, Statecraft, Deterrence, and Defence*. Washington: Center for European Policy Analysis.

Kamizela, D. (2019). F-35 Lightning II – Polski Wybór. *Nowa Technika Wojskowa*, *9*, 6–17.

Matuszewski, M. (2016). Niebieskie ludziki. Wojna morska na Bałtyku nie jest nierealna. Retrieved from https://wszystkoconajwazniejsze.pl/maciej-matuszewski-niebieskie-ludziki-wojna-morska/

Murphy, M., Hoffman, F. G., & Shaub, G. (2016). *Hybrid Maritime Warfare and the Baltic Sea Region*. Copenhagen: Centre For Military Studies, University of Copenhagen.

Ogrodniczuk, M. (2018, Jul 8). Jaka rola Marynarki Wojennej RP? Część 1. Retrieved from: http://dziennikzbrojny.pl/artykuly/art,2,4,10939,armie-swiata,wojsko-polskie,jaka-rola-marynarki-wojennej-rp-czesc-1

Pacek, B. (2018). *Wojna hybrydowa na Ukrainie*. Warszawa: Oficyna Wydawnicza RYTM.

Piekarski, M. (2019). Hybrid Warfare. *Frag Out! Magazine*, *23*, 46-53.

Shlapak, D. A., & Johnson, M. W. (2016). *Reinforcing Deterrence on NATO's Eastern Flank*. Santa Monica: Rand Corporation.

Tymoczko, J., & Banaś, P. (2019). jednostki-wojskowe.pl [a website]. Retrieved from https://www.jednostki-wojskowe.pl/

Wojnowski, M. (2015). Mit „wojny hybrydowej". Konflikt na terenie państwa ukraińskiego w świetle rosyjskiej myśli wojskowej XIX–XXI wieku. *Przegląd Bezpieczeństwa Wewnętrznego: Wydanie Specjalne*.