Pulaski Policy Papers
Komentarz Międzynarodowy Pułaskiego
ISSN 2080-8852 Warsaw, 26.06.2023

Author: Andrzej Kozłowski

Polish "cyberclaws". Building of the cyberarmy of the rising military power in Europe

Since the outbreak of Russia's large scale invasion against Ukraine Poland procured a significant number of military equipment, which should increase the firepower of the Polish Armed Forces. The Polish Armed Forces also have not forgotten about the development of cyberarmy, which was established in 2018 and should be fully operational by 2026. The question is whether Poland has the potential and will to be a significant power in cyberspace?

> *Cyber components must be integrated into joint warfare and cooperate closely with other branches of Armed Forces*

The beginning

The main drivers behind the creation of the cyberarmy were the increasing threats from cyberspace as more and more countries developed cyber arsenals and used them against other countries as well as NATO decisions made at the Warsaw summit in 2016. The growing role of IT technologies on the battlefield has also made the military become more and more susceptible to possible cyberattacks. NATO member states suffered from cyber operations for example in 2008 when the United States Armed Forces were hacked[1]. Cyber was also used against Estonia in 2007, while in 2008 Russia demonstrated an attempt to integrate cyber into modern war during its attack on Georgia. The growing sophistication of operations aimed at critical infrastructure shows that the threats from cyberspace are only growing. The second important factor, which drove the setting of cyberspace up was the NATO summit in Warsaw in 2016. There the cyberspace was

[1] Operation Buckshot Yankee was a 14-month operation to eliminate the malicious code which was put into a USG port from a laptop in the United States Central Command. It was one of the most serious incidents in the history of the US military.

declared as the next operational domain and countries based on Article 3 of Washington Treaty[2] are obligated to develop capabilities to operate in a digital environment.

The first concept of Polish cyberarmy was presented by Minister of Defence Antoni Macierewicz during the Cybersec conference in 2018. He announced the plan to create a unit consisting of 1000 soldiers. However, this plan was stopped and eventually buried when Macierewicz was dismissed and replaced by Mariusz Błaszczak. However, the process of creating a cyberarmy was soon restarted. On 2nd May 2019 Minister Błaszczak nominated general Karol Molenda as plenipotentiary for the creation of cyberspace defence forces. His first step was a consolidation of the different military entities responsible for cybersecurity. The National Centre of Cryptology and the IT inspectorate were merged into the National Cyber Security Centre.

Cyber Command of Polish Cyberspace Defence Forces

On 8th February 2022 there was a next milestone in the development of the Cyber forces of the Polish Armed Forces when the Cyber Command was set up and Polish Cyberspace Defence Forces were also officially created. The Cyber Command is tasked with supervising the tactical units. The previously existing National Cyber Security Centre was renamed as National Cyber Security Centre – Command of Cyberspace Defence Forces. There are around 5 thousand military and civilian personnel working for this structure including hundreds of cybersoldiers, though the exact number remains secret. The recruitment process is still open.

Polish Cyberspace Defence Forces, which will be fully operational by 2026, will become a specialist component of Polish Armed Forces on the basis of the Homeland Defence Act, which was introduced after the Russian large scale invasion of Ukraine and was aimed at strengthening the Polish Armed Forces. The process of creation of the Polish Cyberspace Defence Forces is based on the experiences from the Polish Special Forces creation, which at the beginning was also a specialist component of Polish Armed Forces to be later transformed into a separate military branch.

Polish Cyberspace Defence Forces in time of peace will be directly subordinate to the Ministry of Defence and in time of mobilisation and war they will be directly subordinate to the Commander-in-Chief selected by the President. Polish Cyberspace Defence Forces are responsible for securing cyberspace and are capable of conducting the full spectrum of operations including defensive,

[2] The Article 3 of The North Atlantic Treaty: “In order more effectively to achieve the objectives of this Treaty, the Parties, separately and jointly, by means of continuous and effective self-help and mutual aid, will maintain and develop their individual and collective capacity to resist armed attack”.

reconnaissance, and offensive as well as counteracting against psychological and information operations.

The unit is responsible for:

- Ensuring the cybersecurity of the Ministry of Defence,
- Planning, organising, operationalising and using cyberspace;
- Conducting operations in cyberspace;
- Building, maintaining and protecting infrastructure and information in cyberspace;
- Providing support for military operations conducted by the Polish Armed Forces and operations conducted within alliance and coalitions;
- Coordination with other state institutions responsible for defence;
- Conducting research and preparing innovative solutions for detecting incidents in cyberspace;
- Projecting, building, implementing and using national cryptologic technologies and solutions to assure information security;
- Producing new solutions in area of modern technologies and cryptography;
- Conducting educational activities;
- Supervising the work of CSIRT MON, which is responsible for monitoring MOD networks 24/7 and defending Polish cyberspace.

Cyber Offensive capabilities

The interesting aspect of every cyber unit in the military is its ability to conduct offensive operations. Polish Cyberspace Defence Forces are restrained in commenting on this issue but the officials declare that Cyberspace Defence Forces will be able to conduct all spectrum of operations in cyberspace including offensive operations. Such actions were undertaken first time during the NATO military exercise in 2016 Anakonda-16, when cybersoldiers conducted phishing attacks. The results of these drills are unknown to the public. Commander of Polish Cyberspace Defence Forces General Karol Molenda also claimed that new unique tools were being developed by the army including offensive ones.

The great problem - lack of staff

The Polish cyber military forces share the same problems as almost every military, which intends to develop its own cyber units. They struggle to find suitable candidates for service as there are not enough people with the cybersecurity skills on the market and thus, private sectors attract them with much more competitive salaries. Therefore the Polish Armed Forces want to solve this problem two-fold. They created a special Military IT High School in Warsaw, which should prepare

candidates for the Military University of Technology to study IT, cryptology or cybersecurity with the enrolment number for cybersecurity specialisation increased as well. Also schools for non-commissioned officers were opened to produce candidates who specialise in IT and communication. The educational component was later developed by setting up of the Cybersecurity Summer Schools and creating classes with the profile “Cybersecurity and modern IT technologies” in 16 high schools in Poland. This last idea should increase the number of potential candidates who want to study cybersecurity at the Military University of Technology and later potentially join the army.

Alongside, Poland also followed the idea of the American National Guard and tried to find Territorial Defence Forces volunteers with IT or cybersecurity expertise. These efforts lead to creation of small auxiliary units – Teams of Actions in Cyberspace, which support the Polish Cyberspace Defence Forces. In the time of coordinated efforts, these teams will be taken from Territorial Defence Forces and subordinated to Polish Cyberspace Defence Forces.

Poland also set up a Cyber Security Training Centre of Excellence to improve skills and knowledge of soldiers from various cybersecurity dimensions and teach them to work as a team. Commander of Cyberspace Defence claimed that the commercial market does not offer complementary training preparing cybersoldiers to fulfil tasks in the military and therefore the Cyber Security Training Centre of Excellence is needed. It offers a variety of training and dedicated courses for cybersoldiers in IT, cryptography and cybersecurity.

Not only does the Polish military want to attract more personnel but also maintain the current number of cyber soldiers by proposing additional money. Every cybersoldier receives a special IT financial benefit, which makes his salary closer to those in the private sector. The scale of these benefits depends on the qualifications, experience and position. However, the lack of personnel still is one of the most significant problems and with the worsening demographic situation it will only become more serious.

International cooperation

Polish Cyberspace Defence Forces signed a memorandum of understanding with NATO to create 24/7 points of contact responsible for the coordination of cybersecurity policy and the technical analysis of threats. They also set a framework for a NATO reaction to a significant cyberattack on Poland. What is more, the cooperation with NATO Cooperative Cyber Defence Centre of Excellence was established.

Polish Cyberspace Defence Forces also developed bilateral cooperation with the United States in synchronising the military cooperation on cybersecurity and capabilities development in

cyberspace. Also, the agreement on coordination between military CSIRTS was signed with Lithuania. The close cooperation between both countries resulted in the 2nd place in NATO largest cyber exercise LockedShields 2022. The similar agreements were signed also with other countries and especially important is the one with Ukraine as it allows to deepen knowledge about tools and techniques of Russian operators.

The cooperation is also developed with private sector companies such as Microsoft. Polish Cyberspace Defence Forces signed an agreement with Microsoft to join the Government Security Program, which will allow access to source code, information exchange about threats, and early warnings about potential vulnerabilities. 45 countries and international organisations participate in the programme.

Plans for future

The Ministry of Defence has very ambitious targets to further develop cyber components in the Armed Forces. It develops a plan named Cyber Mil 2.0 based on 5 pillars:

- Further development of current cybersecurity structures and infrastructure;
- Education and training;
- Recruitment of new soldiers;
- Building a strong international position;
- Creating and acquiring tools necessary to conduct a full spectrum of cyberspace operations.

One of the most ambitious projects is the creation of the Centre of Joint Operation in Cyberspace, which should consist of the existing units responsible for cybersecurity and military special forces, military police and people responsible in charge of research and development, and training. The Polish MoD also plans to develop the cyber exercise range to make it the largest such object in Europe, where cyber soldiers from allied countries could train and improve their skills.

The military, as part of developing an education domain, plans to open Cyber.Mil Academies at the Universities in small and medium cities. They will get support to develop programmes dedicated to cybersecurity in order to encourage students to join the cyber component of the army. What is more, the Army also plans to open Executive DBA studies for managers who develop their competencies in the cybersecurity area. The next investment is to create a military technological Cyberpark, which should connect the academia with the economic and military sectors. Last but not least, the military also plans to cooperate closer with e-sport to create a military league of Capture The Flag for students of military universities to improve their skills.

A lot of ambiguity

Despite the initial claims that the conception of Polish Cyberspace Defence Forces will be partially available to the public, the enitre document is still confidential and a lot of details are still unknown. The doctrine and strategy of Polish Cyberspace Defence Forces are unknown while many other similar military components from NATO countries are more transparent about it as e.g. Dutch cyber military forces. One of the vital questions is whether the operations of Polish Cyberspace Defence Forces are limited only to the time of war as is the case with most of the cyber forces in European countries or whether it is more flexible and could create cyber space effects in time of peace too, similarly to the US Cyber Command.

Conclusion

1. The decision to create Polish Cyberspace Defence Forces seems natural taking into consideration the role of technology and IT on the current battlefield. The large-scale Russian invasion against Ukraine only confirmed that cyberspace has become the next area of battlefield. It also confirms that the decision to set up a cyber component in the Armed Forces was right as the number of cyberattacks attempts against military systems in 2022 significantly increased in comparison to 2021. Thus, the Polish Cyberspace Defence Forces should continue their development.

2. The Polish Cyberspace Defence Forces must learn the lesson from the role of cyber in the Russian invasion of Ukraine. Therefore, the close contact with Ukrainian counterparts should be continued and developed and Polish cyber units should be engaged into the activities on the cyber exercise range. The frequent training and consultations are vital and allow Polish structures to prepare better against Russian cyberattacks attempts and better understand the role of cyber on the current battlefield. Especially by looking at the example of cyberattack effectiveness but also the limitations of operations in cyber space.

3. The continuation of international cooperation is extremely important as cybersecurity is a team play. It will be important to establish relations with countries such as South Korea, Japan and Taiwan, which have a vast expertise on Chinese cyber groups, which alongside Russian groups are the most daunting challenge for Poland and the Western World.

4. Polish Cyberspace Defence Forces must be more transparent in order to attract more people to join. The scope and tasks should be more elaborate because one of the most common causes of leaving cyber military structures or a lack of interest in serving there is boredom and lack of interesting tasks.

5. Polish Cyberspace Defence Forces will not be able to propose better salaries than private sectors. However, they can create an image of elite prestigious components, which attract people and make them very competitive on the commercial market later.
6. Cyber components must be integrated into joint warfare and cooperate closely with other branches of Armed Forces as cyber serves as an enabler and force multiplier for other forces. It should be practiced during military drills.

Author: Andrzej Kozłowski, Head of Research Office, Casimir Pulaski Foundation

Founded in 2005, the **Casimir Pulaski Foundation** is an independent, non-for-profit, non-partisan Polish-think tank conducting research on different aspects of European and Transatlantic security, with a special focus on Central and Eastern Europe.

The Foundation brings together dozens of international experts in various fields (foreign policy, defence, energy, democratic resilience) and publishes analysis describing and explaining international events, identifying trends in the European and Transatlantic security environment and recommending solutions for government decision-makers and the private sector.

The Casimir Pulaski Foundation is also the initiator and main organizer of the **Warsaw Security Forum** conference, which since 2014 annually gathers over 2000 stakeholders from more than 60 countries in order to elaborate shared responses to common transatlantic security challenges.

Each year the Foundation presents the **“Knight of Freedom”** award to outstanding figures who contribute to the promotion of the values of General Casimir Pulaski, such as freedom, justice and democracy. It is also the home to the Polish branch of the **Women in International Security network.**

The Casimir Pulaski Foundation has been ranked as the **first among Polish Think Tanks** dealing with defence and national security according to the ‘Global Go To Think Tank Index’ report in 2018, 2019 and 2020 respectively. The Foundation also has a status of a partner organization of the Council of Europe.

www.pulaski.pl