Tomasz Zdzikot*

Poland's Path to Building Cyber Capabilities

Abstract

In October 2023, Poland hosted the next edition of the Cyber Commanders Forum, the world's largest conference of military cyber commanders. For the first time, the Forum was hosted by the Polish Cyberspace Defense Forces Component Command. This is a recognition of the international community for Polish achievements, resources and capabilities. The article is a transcript of a speech delivered during the Forum, describing the Polish path to building cyber capabilities, framed in five key success factors.

Key words: Cyber capabilities, Armed Forces, Cybersecurity, Cyberspace, Cyberwarfare

* Tomasz Zdzikot, Member of the Security and Defense Council to the President of the Republic of Poland.

Introduction

In 2018, the Minister of Defense, Mariusz Błaszczak, entrusted me with the task of building the cybersecurity system of the Ministry of Defense. When embarking on this challenging, responsible and extensive project, I first wanted to approach the subject comprehensively, touching all the most important issues in the cyber area. From the perspective of the work on the program, which took the final name CYBER.MIL.PL, I considered five issues to be important: 1) assessing the existing state, taking into account potential, needs and development opportunities; 2) finding the right people to take on the tasks and do it with commitment and professionalism; 3) setting strategic goals; 4) building a communications environment and opening up the military to the outside world; 5) constructing a list of specific projects, initiatives that make up the strategic goals.

Assessment of the existing state. Strengths and weaknesses

Cyberspace is the only operational domain created by man. It is, therefore, man who is its architect and user, both the strongest and potentially the weakest link in the cybersecurity chain. I was, and am, convinced that in Poland's case, human resources are an asset, a competitive advantage and an opportunity, not a problem. For years, Polish pupils, students and mature experts have been among the world's leaders in winning international science Olympiads, especially in mathematics, IT, cryptology and programming competitions and contests. We also have a rich tradition associated, for example, with breaking Bolshevik cyphers during the Polish–Russian war, which we won in 1920, or deciphering the German Enigma cypher machine.

The extensive and comprehensive structure of units with different purposes, touching both the operational and training or educational spheres, should also be considered a unique potential of the Ministry of National Defense. Under the authority of the Minister of Defense are military special services, the Military Police, units responsible for communications, IT, cryptology and cybersecurity, as well as, for example, universities.

On the other hand, the dispersion of structures and the unclear division of their responsibilities caused numerous competence problems. Subordinate

units were exchanging letters instead of focusing on achieving goals. The structure lacked key links, such as a military CERT and a centralized cyberspace defense command.

People

Here, I was very lucky. I managed to gather around a problematic and multifaceted project a group of excellent people – officers of the Polish army, officers of the special and uniformed services, and civilians, including scientists. I have always been close to Albert Einstein's maxim, „Everyone knows that something can't be done, that it's impossible until you find someone who doesn't know that, and he just does it". I found such people. Within two years, we did the work that, under normal circumstances, the military bureaucracy would have spread out over 20 years. It would be possible to mention by name a great many people to whom Poland owes a vast leap forward in the area of military cyber. The success of the Polish way is chiefly due to the formation within the Ministry of Defense, the Polish Armed Forces, the special services and military universities, bringing together a group of dedicated professionals, thanks to whom we can today tell a story of success that has many fathers and mothers.

Strategic objectives

We decided to organize our activities into several strategic objectives, which will then be filled with content by creating a list of the projects that comprise them. Taking into account the challenges coming from our country's security environment, the analysis of the potential and current situation and needs, as well as being in line with the goals of the nationwide cyber security strategy, the CYBER.MIL.PL program was therefore divided into four pillars. The first was to consolidate and build cybersecurity structures; the second, education, training and exercises; the third, cooperation and building a strong international position; and the fourth, raising the security level of the military networks and systems. This approach, on the one hand, organized the work, but more importantly, it communicated our long-range intentions and showed all stakeholders the direction in which we were heading. In this way, the strategic goals also played a role in inspiring a creative quest for activities and projects that fit this overall framework.

Communications

When we started, the Ministry of National Defense and the Armed Forces were unfortunately not commonly associated with cyber activity. This, in turn, posed a significant limitation in the ability to attract staff to serve, cooperate, or pursue military studies in fields related to the cyber domain. When competing with the private sector, the military cannot rely solely on financial incentives. Of course, the system of financial allowances for cyber experts created first by our team in the military, and then at the government level, for the entire public sector, already makes it possible to offer particularly valuable people salaries that are not out of line with market realities. However, other incentives should also be actively used. In the case of the military sector, they are not difficult to identify. One may be the high social prestige of military service and service in guarding national security. For it to be treated as such, however, the military must make a communicative effort to interact with the outside world and use all kinds of tools – hackathons, social media, picnics, festivals, and traditional media. It must be present where people gather and meet their questions. In this way, it can be shown that service in the cyber component of the armed forces offers the opportunity for continuous development, exceptional training, exercises, international relations, or, finally, to touch areas unattainable anywhere else, including constant interaction with a well-prepared and highly motivated adversary.

List of projects

It is difficult at this point to list the projects already implemented or still being implemented as part of the continuation of the CYBER.MIL.PL program. There were several hundred of them. I consider the institutional ones to be extremely important. This is because I firmly believe that institutions, well-constructed and embedded in the system, are essential to ensure the continuity of the ideas being implemented. Therefore, the axis of the program comprised structural reforms leading, in the first stage, to the consolidation of units responsible for cybersecurity, with those dedicated to IT and military networks. The National Center for Cybersecurity was created. It became an incubator for the Cyberspace Defense Forces Component Command, which was ultimately formed. The Cyber Security Training Centre of Excellence was established. It carries out training and exercises in Poland and for the benefit

of allies, in line with the doctrine of continuous improvement of competence and retraining in accordance with the needs and priorities of national security. We have established the Military High School of Information Technology in Warsaw, operating at the Military University of Technology. This is because we believe that the earlier we start educating recruits for future military service, the better and more consistently educated they will be. The equivalent purpose was served by the „CYBER.MIL with Class" project, under which in each province, there are, under the auspices of the Ministry of National Defense and the Cyberspace Defense Forces, classes at the high school level with a profile in cybersecurity and modern information technology.

A CSIRT of the Ministry of Defense was established as an essential component of the national cybersecurity system. We also took care of the expert base by creating the Maritime Cyber Security Center at the Naval Academy in Gdynia and the Academic Centre for Cyber Security Policy at the War Studies University in Warsaw. Much attention has been paid to education. In addition to programs for high school students, we have decided to raise enrollment limits for military studies in cyber and IT-related fields by several hundred percent. Military universities have also launched specialized postgraduate programs and excellent specialized MBA programs in cybersecurity dedicated to both military and civilian managers. We have added a cyber component to the voluntary military training program for students. Moreover, a Cyber Operations Team in the Territorial Defense Forces has also been formed, allowing cyber experts to combine their professional work in the private market with military service.

Due to the nature of cyber threats, which are always cross-border, much attention has been paid to building international relations. This is an opportunity to exchange good practices and experiences and to act faster and more comprehensively in case of cybersecurity incidents. That is why in 2018, we signed a Memorandum of Understanding (MoU) between the Polish government and NATO on cooperation in the area of cybersecurity defense. In 2019, an extremely important Polish–US agreement on cyberspace cooperation was concluded, preceding the conclusion of agreements with other allies, such as South Korea.

As regards the security of the military networks and systems, it is difficult to discuss specifics covered by secrecy clauses. However, our activities generally focused on technical projects, guaranteeing their integrity and confidentiality.

Summary

According to the Polish legal system, the Minister of Defense is in charge of handling incidents during martial law. This task requires that the structures subordinate to the minister, including, in particular, the Cyberspace Defense Forces, cooperate continuously with all stakeholders involved in the national cybersecurity system. Only by doing so will it be possible to take effective action. From the perspective of industry and business, it is also an opportunity to benefit from the knowledge and experience of the Armed Forces and to participate in joint exercises and training. This is why an increasing number of large Polish companies are entering into cooperation agreements with the Cyberspace Defense Forces. This is the right and natural step for all organizations to be aware of the risks associated with the digital world.

The path we have traveled has been recognized. In the „The Cyber Defense Index 2022/23", Poland was ranked 6th globally. We gave way only to Australia, the Netherlands, South Korea, the US and Canada. It is worth noting that the ranking was published in the pages of the American magazine „MIT Technology Review", founded in 1899 by one of the world's top technical universities – the Massachusetts Institute of Technology (MIT), and was based on a global survey featuring 1,000 senior managers conducted by the magazine. As for Poland, the role and importance of the Cyberspace Defense Forces, created within the program framework discussed briefly above, was recognized and appreciated directly.

Sharing our former experiences and the way we perceive the challenges, we are constantly in action implementing new projects. It should always be remembered that cybersecurity is not a state that can be achieved and maintained but a continuing process of improvement, in constant interaction with adversaries and under increasing pressure.

Droga Polski do budowy zdolności cybernetycznych

Streszczenie

W październiku 2023 roku w Polsce odbyła się kolejna edycja Cyber Commanders Forum, największej na świecie konferencji wojskowych cyberdowódców. Gospodarzem Forum po raz pierwszy było Dowództwo Komponentu Sił Obrony Cyberprzestrzeni RP. Jest to uznanie społeczności międzynarodowej dla polskich osiągnięć, zasobów i możliwości. Artykuł jest zapisem wygłoszonego podczas Forum referatu opisującego polską drogę do budowania zdolności cybernetycznych, ujętą w pięciu najważniejszych czynnikach sukcesu.

Słowa kluczowe: możliwości cybernetyczne, siły zbrojne, cyberbezpieczeństwo, cyberprzestrzeń, cyberwojna