Tomasz Zdzikot*

Capacity building – how to encourage cyber-experts to join the military?

Abstract

One of the biggest challenges faced in building the capacity of armed forces to operate in cyberspace is to attract, improve and retain expert staff. Cyberspace is, after all, the only operational domain that has been entirely created by people, so people have to be able to use it and also to constantly create it anew.

According to the estimates cited e.g. by ENISA in 2019, there was a shortage of over 4 million cybersecurity specialists on a global scale, and approx. 65% of organisations declared staff shortages in the area of tasks related to cybersecurity. A real race for specialists in this domain is observed among both international corporations and domestic companies from plenty of industries, critical infrastructure operators and, finally, intelligence services. In this inter-sectoral, global competition, the public sector (which includes the military) is often in a difficult situation because of the limited possibilities of using financial incentives.

Considering the needs and constraints, a resources-building strategy should be adopted that uses all the advantages found within the range of influence of the military sector. The article discusses them using various approaches, based on actions successfully implemented by the Polish Ministry of National Defence under the programme of capacity building in the armed forces to operate in cyberspace. The first aspect the image, motivation and challenges. Service in the cyber armed forces component provides the opportunity to reach areas unattainable anywhere else, including constant interaction with a well-prepared and highly motivated enemy. The second point for consideration is education and continuous improvement. The possibilities to recruit experts who already have a good position in the commercial market are limited. Therefore, development of the

* Tomasz Zdzikot, Secretary of State at the Ministry of National Defence and Plenipotentiary of the Minister of National Defence for Cyberspace Security (2018–2020), responsible for the creation and implementation of the CYBER.MIL.PL programme.

military education system is the best way to ensure a steady inflow of staff. In Poland, it was decided both to use military academies for this purpose and a real educational ecosystem is being created and constantly developed, also including a military IT secondary school and a dedicated non-commissioned officer school. Civilian secondary schools run (in co-operation with the Ministry of National Defence, MON) profiled vocational training classes, students of civilian universities undergo military training in cybersecurity, and the performance improvement will be managed by the Expert Cybersecurity Training Centre. The third aspect is the Territorial Defence Force, which gives the opportunity in the Cyberspace Operations Team to combine military service and to continue previous professional work on an extremely competitive market.

Key words: cybersecurity, armed forces, Ministry of National Defence

Why and how does the Ministry of National Defence acquire expert staff?

One of the biggest challenges faced in building the capacity of the armed forces to operate in cyberspace is to acquire, improve and retain expert staff in the service. Cyberspace is, after all, the only operational domain that has been entirely created by people, so people have to be able to use it and also to constantly create it anew.

According to the estimates cited, e.g., by ENISA in 2019, there was a shortage of over 4 million cybersecurity specialists on a global scale, and approx. 65% of organisations declared staff shortages in the area of tasks related to cybersecurity. Consequently, 51% of organisations assessed that this made them exposed to the risk of security breaches[1].

A real race for specialists in this domain is observed among both international corporations and domestic companies from many industries, critical infrastructure operators and, finally, intelligence services. In this inter-sectoral, global competition, the public sector (which includes the military) is often in a difficult situation because of the limited possibilities of using financial incentives.

Considering the needs and constraints, a resources building strategy should be adopted that uses all the advantages found within the reach of impact of the military sector. It was on this assumption that the Polish Ministry of National Defence developed the programme of capacity building in the armed forces to

1 Report "Cybersecurity Skills Development in the EU", prepared by ENISA in December 2019 – https://www.enisa.europa.eu/publications/the-status-of-cyber-security-education-in-the-european-union.

operate in cyberspace called CYBER.MIL.PL, which it has been implementing successfully since 2018 and presented to the public in February 2019.

Thus, first of all, the importance of image, motivation and challenges was taken into account in the recruitment process, as well as at the pre-recruitment stage, related to building the recognition and brand of the cyber component of the Armed Forces of the Republic of Poland. This type of military service offers a special opportunity to reach some fields unattainable anywhere else, including constant interaction with a well-prepared and highly motivated enemy.

Second issue under consideration is education and continuous improvement of staff. The possibilities to recruit experts who already have a good position in the commercial market are limited both due to the aforementioned general scarcity of highly qualified resources, and due to constant pay disproportions[2]. Therefore, from the perspective of the Ministry of National Defence, which has its own facilities and training capabilities, the development of the military education system is the best way to ensure a steady inflow of staff. Interestingly, the Ministry uses for this purpose both military academies and creates a real educational ecosystem, also including a military IT secondary school and a dedicated NCO school. Moreover, civilian secondary schools run (in co-operation with the Ministry of National Defence) profiled vocational training classes, students of civilian universities undergo military training in cybersecurity as part of the "Legia Akademicka" programme, while performance improvement will be managed by the Expert Cybersecurity Training Centre being established.

The third aspect is the youngest, fifth type of the Polish Armed Forces, i.e. the Territorial Defence Force, allows combining professional work on the civilian market with military service, also in cybersecurity – in the Cyberspace Operations Team.

2 According to analysts, the average remuneration of an IT security officer individually responsible for cybersecurity in 2019 in a company employing up to 300 employees was from PLN 16,000 to 20,000 per month. On the other hand, in larger enterprises, a leader in a team of 2–3 could expect a salary of PLN 20,000–25,000 per month, https://biznes.interia.pl/praca/news-poszukiwani-specjalisci-ds-cyberbezpieczenstwa,nId,2988175.

Statutory tasks of the Minister of National Defence in capacity building

The range of operations of the government administration department of national defence, headed by the Minister of National Defence, in a time of peace covers the issues of cyberspace security in the military dimension. Simultaneously, the computerisation department deals with cyberspace security matters in the civilian dimension[3]. Thus, the legislator clearly separates the military area, related to the activities of the Ministry of National Defence and the Armed Forces of the Republic of Poland, and the development of the ability to conduct independent or allied operations, starting from the widely understood civilian cybersecurity, being a domain of a number of public and private sector entities and units. It should be emphasised that the above-mentioned distinction introduced into the structure of government administration departments was not, in fact, necessary under the provisions of the Act on the National Cybersecurity System. As implied from the entirety of applicable standards, the issues of state defence and the Armed Forces of the Republic of Poland can be governed in the Council of Ministers by the Minister of National Defence only[4]. Nonetheless, such an unambiguous division created a clear and unambiguous basis for action for the Minister of National Defence. As rightly stressed by legal commentators, "consideration of cyberspace security in the military dimension in the national defence department will allow including cyberspace security issues in the strategic, planning and training documents related to the organisation of the armed forces"[5].

The expression of this generally defined range of jurisdiction is the Act on the National Cybersecurity System, which in Section 10 lists the tasks of the Minister of National Defence. The catalogue of tasks contained in the provisions of Article 51 and Article 52 of this Act is closed, yet it is non-exhaustive. For

3 Pursuant to Article 12a par. 1 (10) and Article 19 par. 1 (1a) of the Act of 4 September 1997 – Governmental Departments Act (consolidated text, Journal of Laws of 2020, item 1220).

4 In particular, Article 134 par. 2 of the Constitution of the Republic of Poland stating that "The President of the Republic, in times of peace, shall exercise command over the Armed Forces through the Minister of National Defence" and Article 19 par. 1(1) of Governmental Departments Act classifying the defence of the State and the Polish Armed Forces as "national defence".

5 *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, red. A. Besiekierska, Warszawa 2019, p. 231.

instance, it does not take into account the liability for running CSIRT MON[6], being one of the pillars of the system established on the basis of the Act. In the context of capacity building and forming the necessary human resources, the essential dispositions are contained in Article 51 (2–4), which provides that the Minister of National Defence is responsible for the following: 1) providing capabilities of the Armed Forces of the Republic of Poland in the national, allied and coalition system to carry out military operations in the case of cybersecurity threats necessitating defence actions; 2) developing the capabilities of the Armed Forces of the Republic of Poland in cybersecurity through the organisation of specialised training projects; 3) acquiring and developing tools for building cybersecurity capabilities in the Armed Forces of the Republic of Poland.

As emphasised by legal commentators, most of the tasks of the Ministry of National Defence, as defined in Article 51 of the Act on the National Cybersecurity System, are the basis for undertaking non-executive actions "in ensuring the efficient functioning of state defence and security in the case of cybersecurity threats"[7]. In the approach that, in the author's opinion, puts emphasis on the area related to the functioning of CSIRT MON, the purpose of the activities of the Minister of National Defence (according to some legal commentators) is to ensure the proper analysis of threats, including incidents, and taking adequate steps to achieve a satisfactory status of cybersecurity[8]. The provision of the Armed Forces of the Republic of Poland with the ability to carry out military operations requires both the organisation of specialised training and exercises, as well as the necessary technical and human resources. The key importance in this scope is of the task described as acquiring and developing tools for building cybersecurity capabilities in the Armed Forces of the Republic of Poland. It is rightly pointed out that it can be considered as a "a task within the realm of activities of a public administration body and will constitute in this context a sufficient legal basis for the performance of civil law

6 Pursuant to Article 12 par. 2 of the Act of 5 July 2018 – Governmental Departments Act (consolidated text, Journal of Laws of 2020, item 1369). CSIRT MON is the "Computer Security Incident Response Team operating at the national level, run by the Minister of National Defence".

7 *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, red. W. Kitler, F. Radoniewicz, J. Taczkowska-Olszewska, Warszawa 2019, p. 301.

8 *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, red. G. Szpor, A. Gryszczyńska, K. Czaplicki, Warszawa 2019, p. 301.

activities"[9]. Therefore, it is obvious that the needs related to ensuring security and conducting operations in cyberspace in subsequent editions of the Plan of Technical Modernisation of the Armed Forces of the Republic of Poland (PMT) are taken into account. Both in the PMT to 2026 approved in February 2019[10], and in the PMT for 2021–2035, taking into account 2020, approved in October 2019, the implementation of the cyber.mil programme, as part of which a package of national tools and software will be created that will use the latest Polish cryptographic technologies and will allow the effective defence of Polish cyberspace" was foreseen[11].

Motivation

As mentioned before, in the case of the broadly understood public sphere, which includes the military sector, financial motivation to start work or enter the service cannot be the main and decisive argument. Service for the national security requires determination and will that is triggered by more than financial incentives. The salary level is, obviously, of significant importance and cannot deviate dramatically from the expectations of recruited professionals. Therefore, the Ministry of National Defence has to take the necessary steps also in this field to meet the market realities and increase the chances of acquiring and retaining qualified expert staff. One of the steps meant to face the expectations and changes in the socio-economic environment was the amendment to the Regulation of the Minister of National Defence on allowances to the basic emolument of professional soldiers introduced in February 2020[12]. Pursuant to the amended regulations, professional soldiers serving in specific (crucial from the point of view of MON) military units

9 *Ustawa o krajowym systemie cyberbezpieczeństwa…*, red. W. Kitler, F. Radoniewicz, J. Taczkowska-Olszewska, p. 301.

10 The specified value of PMT is PLN 185 billion, of which the value of the CYBER.MIL programme is PLN 3 billion – https://www.gov.pl/web/obrona-narodowa/plan-modernizacji-technicznej-mapa-drogowa-rozwoju-wojska-polskiego.

11 The value of PMT is PLN 524 billion – https://www.gov.pl/web/obrona-narodowa/524-miliardy-zlotych-na-modernizacje-wojska-polskiego-do-2035-roku.

12 Regulation of the Minister of National Defence of 25 February 2020 amending the Regulation on allowances to the basic emolument of professional soldiers (Journal of Laws of 2020, item 372).

responsible for cybersecurity, cryptology and IT projects[13], belonging to the personnel groups of "cryptology", "cybersecurity" and "development and programming computer science", receive a fixed service allowance for holding the position, as well as a one-time service allowance after the end of each calendar year. The fixed monthly service allowance amounts to PLN 450 to PLN 2,100[14], while the discretionary annual allowance amounts to 100% to 620% of the monthly allowance. Therefore, a soldier with a monthly allowance of PLN 2,100 may receive allowances of even approx. PLN 13,000[15] per year. In the case of monthly allowance, its amount is to be determined taking into account the nature and scope of tasks or activities carried out by the organisational unit, the number of subordinate soldiers and military employees, as well as the degree of the soldier's fulfilment of the assigned tasks or activities, and the soldier's qualifications (§ 26 par. 2 (1) of the Regulation). In turn, the annual allowance is determined taking into account the scope of tasks or activities carried out by the soldier, their degree of difficulty and complexity, as well as the degree of the soldier's fulfilment of the assigned tasks or activities, and the soldier's qualifications (§26 par. 16 of the Regulation). In the light of the Regulation, a professional soldier serving in the specified units can therefore receive PLN 38,200 solely of the dedicated service allowance annually[16]. Of course, the market level of remuneration for individual positions is often higher. Taking into account the overall trending of salaries of professional soldiers, it should be considered that the trend is becoming more and more competitive[17]. There is no similar additional mechanism in the case of civilian employees. However, recruiters of MON state that they try to offer an attractive salary, which is "subject to individual negotiations with a civilian candidate in each individual case and depends on his or her qualifications, experience, as

13 § 26 par. 1 (8) of the Regulation lists Military Unit No. 5949 (Military Unit No. 3860 and the IT Projects Centre).

14 I.e. as at 26.10.2020 – from approx. USD 116 to approx. USD 540.

15 As at 26.10.2020 – approx. USD 3,360.

16 I.e. as at 26.10.2020 – almost USD 9,900.

17 For instance, according to the report "2020 Cybersecurity Salary Survey" issued by Cynet in January 2020, created on the basis of 1,324 questionnaires completed in December 2019 by IT employees dealing with security in three regions: North America, EMEA (Europe, Middle East and Africa) and APAC (Asia Pacific), in the EMEA region almost 2/3 (64%) specialists stated that the annual salary is below USD 50,000. In APAC, salaries of as many as 79% specialists were within this range. In North America alone, only 4% earned less than USD 50,000 a year, while the remaining specialists received USD 51,000 or more. https://go.cynet.com/hubfs/2020-Salary-Survey-Report.pdf.

well as the scope and nature of the proposed duties in the position" [18] also with regard to civilian employees of the Ministry. In this case, also other salary-related elements, such as employment stability with an employment contract, internship bonuses, jubilee awards, reimbursement of study costs, or preferential group life insurance, train travel discounts, or flexible working hours, are emphasised[19].

The crucial point is, however, that the Ministry of National Defence may use more than financial and associated motivations in the process of acquiring and maintaining the key expert staff. All this because work and service in military units responsible for cybersecurity and cryptology is, first of all, a guarantee of the continuous acquisition of new skills and professional experience. It also gives access to the training resources of NATO, both in Poland and abroad. Secondly, it is a challenge related to the sphere of the common good because such is the nature of service that protects the state's security and sovereignty. All the elements above are emphasised by MON better and better in the recruitment process, which seems indispensable in the face of cross-sectoral and cross-border competition both for the experts qualified already and for the promising enthusiasts[20].

18 https://csirt-mon.wp.mil.pl/pl/articles6-aktualnosci/wojsko-polskie-rekrutuje-najlepszych-do-csirt-mon/.

19 Ibidem.

20 For instance, the communication of June 2020, referred to above, concerning recruitment to CSIRT MON, points out that "Work or service in CSIRT MON means mainly the monitoring and defence of the sovereignty of Poland and its interests in the fourth operational domain. It is an everyday, close co-operation with outstanding specialists in cybersecurity, enthusiasts in their profession, which allows, on the one hand, learning from the best, and on the other, acquiring unique, practical experience in the area of cyberspace security. Everyday duties require the performance of tasks in numerous areas – from the co-ordination of activities at the national level (e.g. resulting from the Act on the National Cybersecurity System), through security tests, analysis and assessment of the impact of cyber threats, to the preparation of thematic reports to ensure the security of the entire Ministry of National Defence in cyberspace. The group of experts from CSIRT MON in NCBC takes active part in exercises and training in cybersecurity, and co-ordinates a number of modern, innovative research and development initiatives" – https://csirt-mon.wp.mil.pl/pl/articles6-aktualnosci/wojsko-polskie-rekrutuje-najlepszych-do-csirt-mon/.

Education

From the systemic point of view, profiling, enhancement, and constant expansion and development of military education is the best response to both the needs of the Ministry and the limitations resulting from changes taking place on the market. Military academies, i.e. public universities that are supervised by the Minister of National Defence[21], are of fundamental importance here, and so are their studies for candidates for professional soldiers. Building the capacity of the Armed Forces of the Republic of Poland to operate in cyberspace must be associated with an appropriate increase in the number of jobs and the percentage of professional soldiers in the established military units. After graduation from 5-year military studies and the commissioning of officers after graduation, one can expect that the decision of a young person to join the army was deliberate and is a conscious choice of the life path for many years, not for a moment. Out of five military academies, two – the Military University of Technology in Warsaw (MUT) and the Polish Naval Academy in Gdynia (PNA) – currently offer military studies with specialisations related to the broadly understood digital domain. In the MUT, these are cryptology and cybersecurity, IT, electronics and telecommunications, and in the PNA – IT and information systems in security. It is worth noting how the reality of operation of military academies has changed in the last few years, which translated into the possibility of their strong involvement in the process of building human resources also in the corps of cryptology and cybersecurity, and communications and information technology. In the academic year 2012/2013, the limit of students in the courses for candidates for professional soldiers amounted to 470 in total in the four military academies offering such studies. In this group, the studies in the discussed specialisations were offered by the MUT only, with a limit of admissions amounting to 102 in electronics and telecommunications and 20 in IT. The admission limit for the entire Polish Naval Academy was 25 midshipmen in total[22]. In the academic year 2015/2016, the total number of places in all academies was 522, including in the MUT: electronics and telecommunication – 84, IT – 47 and, for the first

21 Article 433 par. 1 (1) of the Act of 20 July 2018 Law on higher education and science (consolidated text, Journal of Laws of 2020, item 85).

22 Regulation of the Minister of National Defence of 12 October 2011 on the limits of places in study programmes for candidates for professional soldiers in individual military higher education institutions (ibidem of 2011, no. 226, item 1363).

time, cryptology and cybersecurity with the limit of 15 places. Specialist digital studies were still conducted in the MUT only, with a total of 146 places, while the total limit of admissions to the PNA in Gdynia was 28 midshipmen[23]. Currently, the admissions limit planned by the Minister of National Defence for the academic year 2020/2021 totals 1461, of which in the MUT: electronics and telecommunications – 222, IT – 107, and cryptology and cybersecurity – 116, while in the PNA in Gdynia: information systems in security – 40 and IT – 15. Therefore, 500 of cadets can start education in two military academies in courses related to cybersecurity, cryptology and IT [24]. Since 2015, the total limit of admissions to military studies has almost tripled – from 522 to 1461 (in the PNA in Gdynia, the number is higher by more than 450% – increased from 28 to 130), while in the studies with digital specialisations, the increase is from 146 places to 500, so by over 340%. Of course, we should bear in mind that military studies are 5-year studies because it is only possible to be enlisted for permanent service in the professional officers corps after obtaining the professional title of MA/MSc or equivalent[25], so the effects of increasing the admission limits are considerably postponed. However, such far-reaching changes in admission limits can be considered a systemic solution by which the Ministry determines that the development of the existing units, whose mission is to conduct operations in cyberspace and also to form the Cyberspace Defence Force[26], in the officer corps is to be based on staff educated in the military academies subordinate to MON. As the Ministry informed, the concept of the organisation and functioning of cyberspace defence force, approved in September 2019, assumes that their command will be established by 2022, while the completion of the formation and achievement of the ability to conduct cyberspace operations in the full spectrum is planned for 2024. It

23 Regulation of the Minister of National Defence of 21 November 2014 on the limits of places in study programmes for candidates for professional soldiers in individual military higher education institutions (ibidem of 2014, item 1723).

24 Regulation of the Minister of National Defence of 2 September 2019 on the limits of places in study programmes for candidates for professional soldiers in individual military higher education institutions (ibidem of 2019, item 1738, as amended).

25 Article 11 par. 1 of the Act of 11 September 2003 on the military service of professional soldiers (consolidated text: ibidem of 2020, item 860).

26 By Decision No. 17/MON of 5 February 2019, the Minister of National Defence appointed the Representative of the Minister of National Defence for the establishment of the cyberspace defence force, whose task is, among others, to co-ordinate projects related to the creation of the cyberspace defence force and supervision over the correct implementation of tasks related to the achievement of operational readiness by the cyberspace defence force (Journal of Laws of MON 2019, item 23).

is also clearly emphasised that, by that time, a total of approx. 2,000 graduates of cybersecurity-related courses, who are the basic human resources to be involved in security in cyberspace, should have graduated from military academies[27].

Assigning a leading role to self-education of staff based on military academies, being structurally and substantively justified, also entails the necessity to ensure the best possible preparation and predisposition of candidates for admission to military studies and then to service in the vulnerable sector of cybersecurity. Therefore, under the CYBER.MIL.PL programme, the Ministry of National Defence also develops a specialised educational proposal dedicated to young people from secondary schools. The establishment of the first Military IT Secondary School in Warsaw, at the Military University of Technology, in February 2019 is of prime importance in this regard[28]. The four-year secondary school, given the name of "Polish Cryptologists"[29], with the Minister of National Defence as its governing body, has already had two school year inaugurations. The first recruitment, in which more than 500 candidates applied for 50 places, turned out to be a success[30]. Secondary school education, the main goal of which is to prepare candidates for specialised military studies, is carried out in close cooperation with the Faculty of Cybernetics of the MUT and with the National Cyberspace Security Centre. The curriculum includes advanced mathematics, physics and computer science, but also physical education and military education. What is important, regardless of the place of residence, students are accommodated in a dormitory. Uniforms are also obligatory. Accommodation, meals, uniforms and medical care are free of charge[31].

The second project with the same objective consists in the implementation of "Program CYBER.MIL z klasą", with the pilot carried out in 2019, and full

27 *Tworzymy wojska obrony cyberprzestrzeni*, https://www.gov.pl/web/obrona-narodowa/tworzymy-wojska-obrony-cyberprzestrzeni.

28 Order of the Minister of National Defence No. 5/MON of 18 February 2019 on the establishment of the Military Comprehensive IT Upper Secondary School in Warsaw (Journal of Laws of MON 2019, item 24).

29 Decision of the Minister of National Defence No. 136/MON of 5 October 2020 on assigning the name to the Military IT Secondary School in Warsaw (ibidem 2020, item 158).

30 https://www.bankier.pl/wiadomosc/500-kandydatow-do-Wojskowego-Ogolnoksztalcacego-Liceum-Informatycznego-7672549.html.

31 https://www.wat.edu.pl/aktualnosci/wojskowe-ogolnoksztalcace-liceum-informatyczne-rozpoczelo-swoj-pierwszy-rok-szkolny/.

implementation has been carried out since April 2020[32]. Pursuant to the ordinance establishing the programme, its main objective is "to build a base for recruitment to the corps of professional and scientific staff of the Armed Forces of the Republic of Poland for the needs of organisational units of the Ministry of National Defence, including the planned Cyberspace Defence Force, in IT and ICT security"[33]. The specific objectives explicitly mention "an increase in the number of candidates for military and civilian studies in IT, cryptology and cybersecurity with appropriate IT preparation, intended for the Armed Forces of the Republic of Poland and specialised organisational units of the Ministry of National Defence"[34]. The programme is a pedagogical experiment consisting in creating classes with a curriculum profile "Cybersecurity and modern information technologies" in 16 secondary schools qualified to participate across the country. As part of the profiled curriculum to be implemented in the first 3 school years, the basics of cryptography, history of cryptography, basics of algorithmics, basics of cybersecurity, data and information security management are planned. Students are going to learn about contemporary digital threats, cybersecurity risk management, information systems security and the cryptographic aspects of data protection. From the point of view of the school participating in the programme, it is both an opportunity to modernise the educational proposal and increase the chances of students to take up prestigious studies and develop their careers, and to obtain additional funding. The programme assumes that even 80% of the implementation costs will be covered from the targeted subsidies granted by MON to the bodies governing the schools with cybersecurity classes. Funds from the subsidy can be used for purposes related to remuneration for the teachers of specialist subjects and for equipping and operating IT laboratories, in particular for the purchase of computer hardware, printers, interactive boards, multimedia projectors, licenses and software, trade literature, or the provision of Internet services. In spite of the high requirements set for potential partners, over 30 schools applied for participation in the programme, out of which 16 were eventually selected, one in each Province[35].

32 Order of the Minister of National Defence No. 12/MON of 23 April 2020 on the implementation of the "Program CYBER.MIL z klasą" programme (Journal of Laws of MON 2020, item 73).

33 Appendix to Order of the Minister of National Defence No. 12/MON of 23 April 2020, p. 2.

34 Ibidem, p. 2.

35 https://ncbc.wp.mil.pl/pl/articles6-aktualnosci/program-cybermil-z-klasa/.

The programme of voluntary military training of civilian students "Legia Akademicka" has been an important part of the educational ecosystem of the Ministry of National Defence for several years. The programme is carried out on the basis of an agreement concluded between the Minister of National Defence and the Minister of Science and Higher Education. University rectors benefiting from the support of patronage military units, are the organisers of the theoretical part of voluntary student training, including subjects in defensive capability and military knowledge. The practical part including the basic module and, possibly, also the non-commissioned officer module, takes place during the summer holiday season and is conducted by the Ministry of National Defence as part of military exercise. From 2019, the training module of Legia Akademicka was extended with cybersecurity component implemented by the National Cyberspace Security Centre for a selected group[36]. In 2020, 76 best students from all over Poland studying in faculties such as cybersecurity, IT and mathematics were qualified to specialised training[37].

MON also addressed a proposal to university students at the Bachelor's, Master's and PhD level, aimed at stimulating scientific interest in cybersecurity and cryptology, by setting up in 2019 The Marian Rejewski Award for the best Engineer's, Bachelor's, Master's thesis and doctoral dissertation concerning cybersecurity and cryptology. In the first edition, the award pool was PLN 39,000, of which PLN 8,000 is dedicated to the authors of the best Engineer's, Bachelor's or Master's thesis, and PLN 10,000 for the author of the best PhD dissertation[38]. In the second edition, the total sum of awards was increased to PLN 43,000[39], out of which PLN 12,000 was allocated to the author of the best PhD dissertation[40]. The diversification of scientific disciplines and research

36 Pursuant to the provisions of § 7 par. 1–3 of the Decision of the Minister of National Defence No. 7/MON of 20 January 2020 on the "Legia Akademicka" programme of voluntary military training of civilian students (Journal of Laws of MON of 2020, item 9), specialised training on cybersecurity is addressed to interested civilian students who have successfully completed the non-commissioned module and were promoted to the rank of reserve corporal. The participants are selected by the Director of the National Cyberspace Security Centre in co-operation with the Chief of General Staff of the Polish Armed Forces. The training itself is conducted by the Director of the National Cyberspace Security Centre, in consultation and in co-operation with the Commander of the Territorial Defence Force in the premises of the Communications and IT Training Centre.

37 https://www.cyberdefence24.pl/legia-akademicka-2020-szkolenie-komponentu-cyber.

38 https://www.cyber.mil.pl/edycjai/.

39 I.e. as at 26.10.2020 approx. USD 11,000.

40 I.e. as at 26.10.2020 almost USD 3,100.

areas was noticeable in the first edition. Out of numerous valuable and very interesting proposals, the ones with the highest rate were as follows: the Master's thesis titled "Praktyczne metody wykrywania podatności w kodzie źródłowym (Practical methods of detecting vulnerabilities in a source code)" and the PhD dissertation titled "Wykorzystanie technik eksploracji danych do wykrywania działań nieuprawnionych w sieciach sterowanych programowo" (Using data mining techniques to detect unauthorised activity in software-controlled networks).

It seems that both graduates of Legia Akademicka and junior scientists taking part in the competition for The Marian Rejewski Award can be particularly valuable human resources for the Ministry of National Defence. Therefore, the development of both initiatives is purposeful and justified perspectively.

The Military University of Technology in 2019 launched MBA studies in cybersecurity management (also under the CYBER.MIL.PL programme) for people with well-established education and professional experience who would like to develop and improve their competences. The mission of the studies is to educate specialists for the Armed Forces of the Republic of Poland, MON, security intelligence and the whole spectrum of knowledge-based economy and information society. The studies are intended to improve the managerial staff's skills through transferring knowledge related to the management of institutions that are part of the State's cybersecurity system, projects and technological aspects[41].

Performance improvement of military and civilian staff will also be the main task of the newly established Expert Cybersecurity Training Centre (CST CoE). In line with the concept approved by the Minister of the National Defence in July 2020, the Centre is to "train and prepare future staff, as well as to raise qualifications of the Armed Forces of the Republic of Poland responsible for the performance of activities in cyberspace. Ultimately, the Centre is also intended to play a role of a unit that consolidates the experts' potential and supports the Minister of National Defence in developing co-operation and shaping the directions of development in cybersecurity, cryptology and IT"[42].

The specific character of the constantly changing cyber domain and constant technological progress force systematic training and professional

41 https://www.wat.edu.pl/ksztalcenie/studia-mba/.

42 https://www.wojsko-polskie.pl/articles/tym-zyjemy-v/2020-07-03m-polska-jest-liderem-regionu-w-obszarze-cyberbezpieczenstwa/.

development of people responsible for all links in the cybersecurity chain of the organisation, the Ministry and State. Even the professional specialist education at a good university is only the beginning of the path through further courses, trainings, exercises and certificates. Both postgraduate studies and the Expert Cybersecurity Training Centre being built in Warsaw are an adequate response to the requirements of the security environment.

The created opportunities for professional development in specialties related to cybersecurity addressed to the non-commissioned officer corps also complement the educational proposal of MON. Thinking about this part of the Armed Forces of the Republic of Poland, the SONDA Non-Commissioned Officer School in Zegrze and Toruń was established on 1 October 2019[43]. As stated in the explanatory memorandum to the draft regulation establishing the new institution, "The need to form a non-commissioned officer school in the Communication and Information Technology Training Centre in Zegrze is closely related to the training of non-commissioned officers for the needs of all Branches of Armed Forces (RSZ) and cyberspace defence force"[44].

Territorial Defence Force

Territorial Defence Force is the fifth, most recently created branch of the Polish armed forces[45]. Until its full operational capability, it is directly subordinate to the Minister of National Defence[46]. It was established on 1 January 2017 under the Act of 16 November 2016 amending the Act on the general obligation to defend the Republic of Poland and certain other acts[47]. Ultimately, the Territorial Defence Force is to be composed of approx. 53,000 soldiers, including approx. 5,000 professional soldiers and approx. 48,000 soldiers of the territorial defence force. As at October 2020, there are approx.

43 § 1 (1) (a) of the Regulation of the Minister of National Defence of 19 September 2019 amending the Regulation on non-commissioned officer schools (Journal of Laws of 2019, item 1833).

44 https://legislacja.gov.pl/docs//507/12324851/12627782/dokument419264.docx.

45 Pursuant to Article 3 par. 2 of the Act of 21 November 1967 on the general obligation to defend the Republic of Poland (consolidated text, Journal of Laws of 2019, item 1541), the Armed Forces include the following branches: the Land Forces, the Air Force, the Navy, Special Forces and the Territorial Defence Force.

46 Article 3 par. 1(4) of the Act of 14 December 1995 on the Office of the Minister of National Defence (consolidated text, Journal of Laws of 2019, item 196).

47 Journal of Laws of 2016, item 2138.

26,000 WOT soldiers, while the plan is to reach the number of 28,500 soldiers by the end of 2020[48]. The basic assumption is to enable combining professional work or running a business with the military service in WOT. Territorial military service lasts from one year to six years[49]. However, the most important aspect is that this type of service is based on rotation or availability[50] so, as a rule, at least once a month for two days off from work[51] or outside the military unit, staying ready to report for service on a rotation basis at the time and place specified by the commander of the military unit[52].

The decision to establish the cyber component in the Territorial Defence Force is a proposal addressed to all those who have the necessary competences, and often a well-established professional position, who are willing and able to devote some of their potential and time for the service in the national security of Poland in the new operational domain.

The first stage of the planned activities consists in the formation of the Cyberspace Operations Team of WOT, operating at the Command of WOT in Zegrze, in which 100 soldiers are to serve, including as many as 90% of volunteers involved in territorial military service[53]. The process of forming the first centrally organised Team, which is later to be supplemented with regional structures, is already under way. As the commanders of WOT emphasise, most of the volunteers are qualified employees of the IT and cybersecurity sector hired, for instance, in banks, as well as academic teachers and IT students[54].

From a strategic point of view, the role of WOT in the ministerial cybersecurity system can be defined as one of a "force provider". This means that the Commander of the Territorial Defence Force will be responsible for the organisation, training and equipment of the force, operating in this area in line with the standards set by the Commander of the Cyberspace Defence Force

48 https://media.terytorialsi.wp.mil.pl/informacje/577005/350-nowych-ochotnikow-w-szeregach-terytorialsow.
49 Article 98j par. 1 of the Act on the general obligation to defend the Republic of Poland.
50 Article 98m par. 1 of the Act on the general obligation to defend the Republic of Poland.
51 Article 98m par. 2 of the Act on the general obligation to defend the Republic of Poland.
52 Article 98m par. 4 of the Act on the general obligation to defend the Republic of Poland.
53 https://www.computerworld.pl/news/Cyberkomponent-WOT,417346.html.
54 https://www.rp.pl/Wojsko/302199909-WOT-tworza-zespol-dzialan-w-cyber przestrzeni.html.

(in the initial stage, by the Director of the National Cyber Security Centre). The use of this force will be preceded by its separation and delegated to the operational control of the Commander of the Cyberspace Defence Force[55].

Conclusion

The process of digitisation of the respective areas of our life, for years recording a dynamic growth, has significantly accelerated as a result of the global COVID-19 pandemic. For the last few months we have been able to observe a technological revolution, triggered by restrictions on direct interpersonal contacts required for epidemiological reasons. All the methods and tools for remote work or online service provision have become an indispensable part of our life, a first-need product for lots of people. It is also a time of trial for all structures and people responsible for ensuring cyberspace security, in which their skills, the adopted system solutions and procedures undergo large-scale testing. Moreover, it is a time of confrontation with all those who attempt (often effectively) to make use of the changed circumstances to engage in cybercriminal, disinformation or intelligence activity. Therefore, the need for experts responsible for cybersecurity will undoubtedly increase, and, thus, the present, already serious, global competence gap will grow. Considering the scope of tasks entrusted and the impact of cyberspace security on the national security in times of peace, crisis, and especially in the battlefield environment during war, the Ministry of National Defence must be the leader in the area of competences, abilities and technological and human potential related to cybersecurity. Taking into account the restrictions resulting from the social and economic reality, and also assuming that people can be both the weakest and the strongest link in the cybersecurity chain, only an extensive, constantly upgraded and improved education, recruitment and personnel policy, using all available options, can be a real support instrument. The actions taken consistently by the Polish Ministry of National Defence since 2018 in staff education and performance improvement, motivation and building a positive

55 https://www.defence24.pl/wot-rozpoczely-formowanie-zespolu-dzialan-cyberprzestrzennych.

image of modern Armed Forces capable of operating in cyberspace, aimed at constructing a coherent ecosystem which can meet various needs, show that the Ministry intends to follow this path.

Bibliography

Literature

Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz, red. A. Besiekierska, Warszawa 2019.

Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz, red. W. Kitler, F. Radoniewicz, J. Taczkowska-Olszewska, Warszawa 2019.

Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz, red. G. Szpor, A. Gryszczyńska, K. Czaplicki, Warszawa 2019.

Legal acts

Rozporządzenie Ministra Obrony Narodowej z dnia 12 października 2011 r. w sprawie limitów miejsc na kierunki studiów dla kandydatów na żołnierzy zawodowych w poszczególnych uczelniach wojskowych, Dz.U. 2011, nr 226, poz. 1363.

Rozporządzenie Ministra Obrony Narodowej z dnia 2 września 2019 r. w sprawie limitu przyjęć na studia na określonym kierunku dla kandydatów na żołnierzy zawodowych w poszczególnych uczelniach wojskowych, Dz.U. 2019, poz.1738, z poźn. zm.

Rozporządzenie Ministra Obrony Narodowej z dnia 21 listopada 2014 r. w sprawie limitów miejsc na kierunki studiów dla kandydatów na żołnierzy zawodowych w poszczególnych uczelniach wojskowych, Dz.U. 2014, poz. 1723.

Rozporządzenie Ministra Obrony Narodowej z dnia 25 lutego 2020 r. zmieniające rozporządzenie w sprawie dodatków do uposażenia zasadniczego żołnierzy zawodowych, Dz.U. 2020, poz. 372.

Ustawa z dnia 11 września 2003 r. o służbie wojskowej żołnierzy zawodowych, t.j., Dz.U. 2020, poz. 860.

Ustawa z dnia 14 grudnia 1995 r. o urzędzie Ministra Obrony Narodowej, t.j., Dz.U. 2019, poz. 196.

Ustawa z dnia 20 lipca 2018 r. – Prawo o szkolnictwie wyższym i nauce, t.j., Dz.U. 2020, poz. 85.

Ustawa z dnia 21 listopada 1967 r. o powszechnym obowiązku obrony Rzeczypospolitej Polskiej, t.j., Dz.U. 2019, poz. 1541.

Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, t.j., Dz.U. 2020, poz. 1369.

Zarządzenie Ministra Obrony Narodowej nr 12/MON z dnia 23 kwietnia 2020 r. w sprawie wdrożenia „Programu CYBER.MIL z klasą", Dz. Urz. MON 2020, poz. 73.

Zarządzenie Ministra Obrony Narodowej Nr 5/MON z dnia 18 lutego 2019 r. w sprawie założenia Wojskowego Ogólnokształcącego Liceum Informatycznego w Warszawie, Dz. Urz. MON 2019, poz. 24.

Budowanie zdolności – jak pozyskać cyberekspertów do służby w wojsku?

Streszczenie

Jednym z największych wyzwań związanych z rozwijaniem zdolności sił zbrojnych do działania w cyberprzestrzeni jest pozyskanie, doskonalenie i utrzymanie kadr eksperckich. Cyberprzestrzeń to jedyna domena operacyjna, która została w całości stworzona przez człowieka i to człowiek musi potrafić ja wykorzystywać, a także stale na nowo tworzyć.

Według szacunków przywoływanych np. przez ENISA, w 2019 roku w skali globalnej brakowało przeszło 4 mln specjalistów od cyberbezpieczeństwa, a ok. 65% organizacji deklarowało braki kadrowe w obszarze zadań związanych z cyberbezpieczeństwem. O specjalistów z tej dziedziny trwa prawdziwy wyścig, w którym udział biorą zarówno międzynarodowe korporacje, jak i krajowe firmy wielu branż, operatorzy infrastruktury krytycznej czy wreszcie służby specjalne. W tej międzysektorowej, globalnej rywalizacji sektor publiczny, do którego zalicza się wojsko, jest często w trudnej sytuacji związanej z ograniczonymi możliwościami stosowania zachęt finansowych.

Biorąc pod uwagę potrzeby i ograniczenia, należy przyjąć strategię budowania zasobów wykorzystującą wszystkie przewagi pozostające w zasięgu oddziaływania sektora militarnego. Artykuł przybliża je wieloaspektowo, bazując na działaniach wdrażanych z sukcesem przez polskie Ministerstwo Obrony Narodowej w ramach programu rozwoju zdolności sił zbrojnych do działania w cyberprzestrzeni. Po pierwsze – wizerunek, motywacja i wyzwania. To służba w komponencie cyber sił zbrojnych daje szansę na dotknięcie obszarów nieosiągalnych gdziekolwiek indziej, w tym na stałą interakcję z dobrze przygotowanym i wysoko zmotywowanym przeciwnikiem. Po drugie – edukacja i stałe doskonalenie. Możliwość pozyskania do służby ekspertów dobrze osadzonych już na rynku komercyjnym jest ograniczona. Dlatego rozwój wojskowego systemu kształcenia to najlepszy sposób na zapewnienie stałego dopływu kadr. W Polsce zdecydowano nie tylko o wykorzystywaniu w tym celu wojskowych akademii, lecz także jest tworzony i stale rozwijany prawdziwy ekosystem edukacyjny, w którym działa też wojskowe liceum informatyczne oraz szkoła podoficerska, cywilne szkoły średnie prowadzą we współpracy z Ministerstwem Obrony Narodowej profilowane klasy patronackie, studenci cywilnych uczelni odbywają wojskowe przeszkolenie z zakresu cyberbezpieczeństwa, a doskonaleniem zajmie się powstające właśnie Eksperckie Centrum Szkolenia Cyberbezpieczeństwa. Po trzecie – wojska obrony terytorialnej, które w Zespole Działań Cyberprzestrzennych dają możliwość łączenia służby wojskowej z kontynuowaniem dotychczasowej pracy zawodowej na niezwykle konkurencyjnym rynku.

Słowa kluczowe: cyberbezpieczeństwo, siły zbrojne, Ministerstwo Obrony Narodowej