Edukacyjna Analiza Transakcyjna 2024, nr 13

https://doi.org/10.16926/eat.2024.13.27

Andrzej BOGDAŃSKI
https://orcid.org/0000-0002-3443-0741
War Studies University, Warsaw
e-mail: a.bogdanski@akademia.mil.pl

Good practices in military cybersecurity training

How to cite [jak cytować]: Bogdański, A. (2024). Good practices in military cybersecurity training. *Edukacyjna Analiza Transakcyjna*, *13*, 455–469.

Abstract

The aim of the article was to determine the impact of good practices in the area of IT on the training of soldiers in the area of cybersecurity. To reach the goal, the author's article characterizes the training centres and forms in the Armed Forces in the area of cybersecurity and determines the impact of a growing number of IT core and dedicated services as well as technical-organisational solutions for command support systems on the process of training offered to soldiers of the army of communications and information technology in the area of cybersecurity. As for his practical goal, the author chose to identify the likely direction of change in the way training is provided in terms of the implementation and expansion of ICT systems and services operated. In his article, the author presents the capabilities that military ICT specialists should achieve in order to perform their tasks effectively, and characterizes good practices used in the ICT support system. The cognitive aim of the article was identifying determinants affecting the process of specialized training of communications and information technology troops in line units. The research problem was formulated by the author in form of the question, "What were the differences between the training of IT specialists in civilian and military environments?"

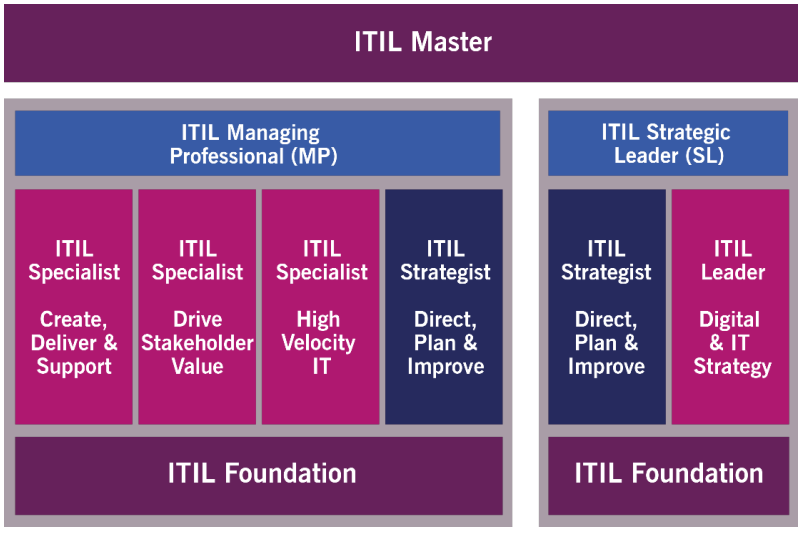
Keywords: good practices, training, cybersecurity, IT, ICT, information security, administration, Help Desk, Service Desk.

Introduction

The Internet and digital Technologies accompanying it have become our inseparable companions. The digital space has also colonized the areas associated

with a clearly human dimension (Borawska-Kalbarczyk K., 2024, p. 49). It is not different in the Armed Forces of the Republic of Poland. ICT systems used by Polish soldiers during peace missions and while training provided services in accordance with the idea of Federated Mission Networking (Bogdański, 2022, p. 49), and were supported by Technology for Information, Decision and Execution superiority. The idea of Federated Mission Networking was based on the code of rules for IT departments, i.e. Information Technology Infrastructure Library. ITIL is a commonly accepted set of best practices developed to support organisations in benefiting from IT services by adjusting them to business strategies. The British government created ITIL in the 80s of the 20th century. At that moment their aim was to define a set of norms, which would allow to improve the efficiency of IT. As time went on, ITIL rules gained popularity and its new versions were released. In 2019, Axelos company released the latest version called ITIL 4, characterized with a more holistic approach to Information Technology Service Management, offering more freedom of adjustment (ITIL Foundation 2018, p. 7). Certification begins with ITIL4 Foundation course, and it could be completed with 5 more trainings and certification exams: ITIL Specialist: Create, Deliver&Support, Drive Stakeholder Value, High Velocity IT. Strategist: Direct, Plan & Improve, Leader: Digital & IT Strategy.

Table no 1
ITIL Master Trainings



Source: https://www.compendium.pl/info/2023/itil-w-wersji-4-juz-dostepny (access: 29.11.2024)

Obtaining the first four certificates results in receiving ITIL Managing Professional title, while the last two in ITIL Strategic Leader title. If a given person ob-

tains both titles and files an appropriate application proving their practical experience in the area of ITIL, showing their long-term participation in practice implementation, there are granted they highest possible title in the hierarchy, i.e. ITIL Master.

The Author of the article posed the research question: How can good practices developed in IT departments of governmental institutions and corporations be used in training future and active soldiers in the armed forces? Activities, and what follows, soldier training differ substantially from processes taking place in the civil environment. The Polish Language Dictionary defines training as a set of lectures from a given subject, organized in order to complete one's education or information from a given field (Słownik, 2024). Thus, in the author's view, the training process in the Armed Forces of the Republic of Poland is a set of activities, a cycle of processes allowing for broadening and gaining further theoretical knowledge and practical skills from a particular field or discipline. IT competencies are already built in uniformed classes from the first stage of acquiring candidates for the Armed Forces (Ostolski, 2020, p. 190). The content of the training addressed to candidates and professional soldiers of the Armed Forces of the Republic of Poland is regulated by appropriate laws, including first of all the act of March 11, 2022 on the homeland defence, which defines candidates' and professional soldiers' preparation for professional military service (Ustawa, 2022, p. 78). Nevertheless, the aforementioned act reads that the training can also take place at universities, schools and training centres other than military.

The aforementioned act provides a general outline of the legal basis for training in the Armed Forces of the Republic of Poland. As for the range of training, with the order on the implementation of the Programme of training of IT and ICT troop subdivisions, Commander-in-Chief of the Armed Forces provided a framework for the training of soldiers already serving in the armed forces in the IT and ICT corps that the author is interested in (Rozporządzenie MON, 2023). The document is intended for subdivisions of IT and ITC troops and constitutes the basis for planning and organizing the training process (Program szkolenia, 2017, p. 2). In the author's opinion, knowledge and skills from the area of cybersecurity should be required from all soldiers, especially those serving in command battalions, which has been emphasized many times by the author during his classes run for candidates for battalion commanders.

The author performed his observations during the biggest military training operations, for instance, those under the code name of Dragon-15, Anakonda-16, Dragon-17, Anakonda-18. The studies presented in the article have also their origin in interviews with experts, conducted by the author as part of the study exercises organised by the Academy of Military Arts in the years 2022-2024. These were the exercises under the code name of Świder-22, Brama Mazowsza-22, Twierdza-23, Świder-23, Brama-23, Twierdza-24. The author's studies realised

during the biggest military training operations show that the main task of a specialized command battalion is achieving and improving their abilities to secure the operation of the command post and to develop and operate ICT command support systems. On the basis of document analysis, interviews and observations, the author concluded that command battalions lacked soldiers specialists of the personal corps of cryptology or cybersecurity, but they only consisted of the aforementioned soldiers of IT and ICT personal corps. These were the soldiers employed at their positions in the ICT Support Centres and selected soldiers operating equipment such as ICT Nodes, Mobile Digital Communications Nodes, Portable and Transportable Satellite Terminals, radio stations. What is more, specialist administrators were employed only in selected command battalions in newly formed administrator teams.

The condition for safe operation of ICT command support systems is appropriate preparation of ICT and IT soldiers, especially in the area of cybersecurity. Sound theoretical knowledge and practical skills of ICT or IT specialists also allow them to gain competence in cybersecurity.

The aim of the article is to define the impact of good practices in the area of IT on soldier training in the area of cybersecurity. To reach his goal, the author's article characterises training centres and forms in the Armed Forces in the area of cybersecurity, and estimates the impact of increasing IT core and dedicated services as well as technical-organisational command support systems solutions on the training process of ICT and IT soldiers.

As for his practical aim (Pelc, 2012, p. 15), the author wanted to identify the likely direction of change in the way of training as far as implementation and development of ICT systems and service operation is concerned. He outlined the capabilities that military IT specialists should achieve in order to performs their tasks effectively, and characterised good practices used in ICT support systems, i.e. Help Desk and Service Desk.

The cognitive aim was to identify determinants influencing specialist training processes of ICT and IT troops in line units. To answer the question, "How can good practices developed in IT departments of governmental institutions and corporations be used in training future and active soldiers in the Armed Forces?" the author presented **the research problem** in form of the question, "What were the differences between the training of IT specialists in civilian and military environments?"

Military and civilian environments

IT specialist training in military and civilian environments differs mainly in its context and specific requirements deriving from the nature of realised tasks. In the military environment, national security is priority. IT specialist military train-

ing should include specialist issues from the area of cybersecurity, defence against cyber attacks, and safe information exchange. The author's studies show that the aforementioned subject matters are not implemented systemically bur only within the framework of in-service training. IT specialists in the army can be engaged in specialist fields such as satellite communication, intelligence analysis, or designing systems supporting military operations. IT military specialists must comply with severe ethical and legal rules, especially in the context of cybersecurity (Ostolski, 2021, p 79). Serving in the armed forces is strictly regulated by state secrets regulations. IT military specialists are trained to fieldwork and are ready to react fast to changing situations. It requires an ability to adjust to different work environments. IT military specialist training often includes using highly-specialised tools and technologies, which are adjusted to unique military requirements. Military IT specialists must understand the organizational structure and decision processes within the armed forces, which is crucial for effective integration of technology and operational goals. Military IT specialists can participate in combat training and simulations in order to test their abilities under near real-life conditions. In the author's opinion, the training should begin with a solid foundation in computer science, including operational systems, computer networks, data bases. IT specialists should be familiar with the latest IT technologies and trends. For obvious reasons, IT specialist training in the civilian environment does not include the content concerning dedicated services used for the needs of building a combined picture of the operational situation. An IT specialist acquired for the Armed Forces from the civilian environment, realizing tasks in the military environment, should complete their knowledge in the area of ICT command support systems and control of combat assets, battlefield simulation systems or specialist services of logistics support.

Training forms

Military IT and ICT specialist training for the needs of improving cyberspace security of the Armed Forces of the Republic of Poland should be realised systemically with regard to the military specialization in ICT corps. The selection of the right candidates should be a very important factor. These are graduates of technical secondary schools, electronic and information technology technicians, specializing in programming, IT, ICT, mechatronics, automation or electronics technology. In the author's view, candidates selected in such a way should be subjected to training in military centres whose division was presented by the author with the help of the act of March 11, 2022 on defence of the homeland.

In the author's view, the main role in the training of future and current personnel should be played by military centres, which can be divided into universi-

ties, non-commissioned officer schools, training centers and units. Among universities there are: War Studies University, Jarosław Dąbrowski Military University of Technology in Warsaw, the Naval Academy, Military University of Aviation in Dęblin and Tadeusz Kościuszko Land Forces Military Academy. During his studies on the training in the area of cybersecurity, the author analysed training programmes in selected non-commissioned officer schools: Non-commissioned Officer School of Land Forces in Poznań, Non-commissioned Officer School of Aviation in Dęblin, Naval Non-commissioned Officer School in Ustka, Non-commissioned Officer School of Military Police in Mińsk Mazowiecki, Non-commissioned Officer School of Special Forces and Sonda Non-commissioned Officer School in Zegrze and Toruń. Moreover, during the research, the following institutions were also operating: Land Forces Training Centre in Poznań, Training Centre of Engineering and Chemical Forces in Wrocław, Artillery and Armament Training Centre in Toruń, Air Force Training Centre in Koszalin, Engineering and Aviation Training Centre in Dęblin, Naval Training Centre in Gdynia, Special Forces Training Centre in Cracow, Artillery and Armament Training Centre in Toruń, and Communications and Informatics Training Centre in Zegrze. Due to high specialization of the military centres, the author described only selected studies and courses in the Military Faculty of the War Studies University in Warsaw, Jarosław Dąbrowski Military University of Technology in Warsaw, and the Communications and Informatics Training Centre in Zegrze.

Training of officer cadres

The War Studies University in Warsaw trains civilian students and it used to educate post-graduate soldiers and qualification course participants. The Higher Staff Course was dedicated to candidates for the position of staff officers of tactical and operational-strategic level with the rank of lieutenant colonel. The aim of the course was preparing officers to take over service positions in command and staff structures of the Armed Forces of the Republic of Poland (AFRP) (Program szkolenia, 2017, p. 2), while the aim of the Battalion Commanders Course was preparing officers to take over positions of battalion commanders or their equivalents. During a 4-month training, the participants of the Higher Staff Course and the Battalion Commanders Course had 10 hours of lessons in cybersecurity, including 4 hours of lectures and 6 hours of classes. The subject matter of cybersecurity was also discussed during classes in ICT and IT, and specialists of the personnel corps of Communication and IT and Cybersecurity, within the curriculum of Command of Types of Forces, additionally discussed cybersecurity during supplementary 30 hours of classes. The author's research also included the analysis of a specialist offer of the Military Faculty which educates also civil-

ian students in the 1st and 2nd degree studies in the field of Command and Defence, and in post-graduate studies in the field of Defence and Security of Cyberspace. Within the framework of specialist training during their 1st degree studies in the field of Command, students learnt about cybersecurity in the Elements of ICT Support in Command course, lasting 40 hours: 10 hours of lectures and 30 hours of classes. On the other hand, within the framework of specialist training during their 1st degree studies in the field of Defence, students learnt about cybersecurity in the courses of Security Basics of ICT Systems Architecture and Fundamentals of ICT networks and systems, 60 hours in total, including 20 hours of lectures and 40 hours of classes, also non-stationary ones. As for the educational aim in post-graduate studies in the field of Defence and Security of Cyberspace, it was to educate military and civilian personnel in the field of cybersecurity to solve problems in the area of security of processed information at different levels of command as well as state command (Program studiów, 2017, p.2). When it comes to specialist post-graduate studies, their basic module offers the courses in ICT Systems and Networks, IT Support of Decision Processes, Hybrid Activity in Cyberspace. What is more, the main module offers courses in Cybersecurity and Protection of Confidential Information and Personal Data.

Moreover, in the offer of post-graduate studies of the War Studies University one could find weekly specialized courses for simulation system operators, i.e. Joint Theatre Level Simulation, a five-day specialized course for technical administrators, and a training scenario in the module supporting exercise management in the Joint Exercise Management Module.

Jarosław Dąbrowski Military University of Technology in Warsaw educates within the framework of civilian, military and post-graduate studies and within the framework courses for the Ministry of Defence. As for the first degree civilian studies, the biggest number of classes concerning cybersecurity could be found in the studying programme for IT specializing in Information Management Systems, Internet Multimedia Technologies, Cryptology, Mobile Computer Systems, ICT Networks and IT Systems. As for military studies in the field of IT, there were three specialisations: Cryptology, ICT Networks and IT Systems. It is worth mentioning the first and second degree studies in Electronics and Telecommunication with their specialization in IT Systems.

The offer of post-graduate studies at the Military University of Technology addressed to junior officers includes the biggest number of classes devoted to cybersecurity in the study programmes in the field of Organisation and Operation of IT Systems for officers meant to take over specialist positions in the area of ICT Systems Operation.

When it comes to courses organized by the Military University of Technology, the biggest number of classes devoted to cybersecurity was included in the course programme for Operating Communication and IT Systems. The course

was dedicated to officers occupying positions in the Command and Communications Support Section at the brigade headquarters. A monthly course in the Administration of ICT Networks and Managing Data Bases is worth mentioning. It was addressed to professional soldiers of the personal corps of communications and information technology who occupied positions in the special division. As for cybersecurity, one might find useful another course in the field of Operating ICT Systems and Network Administration for the soldiers of the personal corps of communications and information technology occupying administrative positions. Another course including the element of cybersecurity was called the Communications and Information Systems of the Armed Forces of the Republic of Poland destined for junior officers of the personal corps of communications and information technology occupying positions in the staff and security divisions. A monthly qualification course called Construction of Military Communications and Information Technology Systems was also precious in terms of cybersecurity content. It was addressed to officers with the second degree university education who planned to take over positions classified to the rank of major in the personnel corps of communications and information technology in the technical personnel group.

Training of non-commissioned officer cadres

The training of non-commissioned officer cadres was also crucial. The author's studies show that the Communications and Informatics Training Centre in Zegrze was leading the way in training NCOs in cybersecurity. The main task of the Centre was training of communications cadres for the needs of the Polish Armed Forces:

— professional soldiers and military workers at professional development courses;
— soldiers in preparatory service;
— students of officers' college;
— non-commissioned officer school students;
— students of the Faculty of Electronics and Cybernetics of the Military University of Technology – participation in training;
— students of the Faculty of Mechatronics of the Naval Academy – participation in training.

The most valuable courses as for theoretical knowledge and practical skills from the area of cybersecurity were those educating in the Administration of ICT Networks addressed to administrators of ICT networks, and development courses regarding the Basics of Windows Operating Systems Administration. The author's observations show that basic courses should be conducted for all IT

specialists, and further specialist courses for particular, selected groups. The scope of knowledge should be closely connected to a given specialisation.

Commercial training

The Communications and Informatics Training Centre in Zegrze significantly modified its offer during the studies in question. Its priority became courses specializing in commercial training based on Cicso company technologies geared at operating services offered in military ICT systems, based on Microsoft's commercial technologies (Bogdański, Zelichowski, 2013, p. 5). As for technologies, Cisco Centrum offered a broad range of certifications and courses focused on various areas of computer networks. The choice of a particular training depended on soldiers' tasks. Here are a few popular Cisco certifications that could be obtained at Cisco Centrum: Cisco Certified Network Associate is a basic certification, directed mainly at persons at the beginning of their career in computer networks. It included basics of configuration, operation and maintenance of Cisco network. Other advanced courses were conducted based on the Expert Cyber Security Training Center and commercial centres. Cisco Certified Network Professional Certification was destined for intermediate network specialists. There were different CCNP paths available, such as Routing and Switching, Security, Data Center, etc. Cisco Certified Internetwork Expert is one of the most advanced Cisco certifications. CCIE concentrated on advanced design, implementations and maintenance skills for wide-area Cisco networks. On the other hand, Cisco Certified Cyber Ops Associate, i.e. the most advanced cybersecurity certification, confirmed the knowledge and skills needed by the teams of Security Operations Center to detect cybersecurity threats and react to them. The Cyber Ops Associate training and exam included the knowledge and skills concerning cybersecurity issues, security monitoring, analysis based on hosts, analysis of network intrusions as well as security policies and procedures. The author's research shows that the training potential of the Communications and Informatics Training Centre in Zegrze ended up with basic courses. Similarly, the centre realised Microsoft technology courses to a limited extent. On the commercial market, training centres offered various courses, both online and stationary, encompassing the area of system, cloud, application management and software development. Here are some basic Microsoft courses and certifications which might be interesting for various cybersecurity professionals: Microsoft Certified Azure Fundamentals is a certification for persons who would like to gain basic knowledge on Microsoft Azure cloud platform. Modern Desktop Administrator Associate is a certification for specialists dealing with Windows systems administration in corporate environment. Microsoft Certified Azure Administrator Associate broadens cloud administrators' knowledge on configura-

tion, management and monitoring of Azure services. Microsoft 365 Certified Modern Desktop Administrator Associate course is dedicated to cyber-specialists dealing with configuration, management and security of Microsoft 365 environment. What is more, knowledge from the field of cybersecurity focusing on detection and reaction to incidents is crucial. Taking into account a broad range of courses, at the beginning of one's professional path the author recommends courses in two basic areas: courses in network and systemic solutions based on Cisco products and courses in server systems and Microsoft services. As for complementing one's knowledge, one should focus on solutions (Bogdański, Barański, 2014, p. 167) from the area of virtualization if they are not based on Microsoft solutions. In each area, there are technology sub-areas and levels. What is more, the research shows that training needs were much bigger than the capacity of military training centres. The research shows that not all soldiers meet minimal requirements as far as basic technical knowledge is concerned. Acquiring candidates from the corps of professional privates can be an efficient and effective solution. The studies also show that a preferred career path in the officer corps was a training limitation. The first position for the academy graduate was a platoon leader. After a three-year term as e. g. a communication or command platoon leader, officers were forced to complete their knowledge gained during their studies as the scope of their professional duties made their current knowledge obsolete, and skills acquired at the academy needed constant practice. A precious source of observation for the author concerning practical skills in the area of using good practices was the preparation process for the biggest practice in the Polish Army in the years 2016–2023 and its realization in the area of ICT support.

Good practices in the area of ICT support

Within the framework of their practice under the code name of Anakonda or Dragon, IT specialist soldiers played the role of Service Desk operators in the Network Operations Center. Service Desk is an organizational unit or a role played by a team of selected people, responsible for functional support of IT applications and IT troubleshooting – both hardware and software. Service Desk is one of the components discussed in the Information Technology Infrastructure Library. The centre of network management is one or more locations where network monitoring, operation or management is performed via a computer, ICT or satellite network. The practice under the code name of Anakonda or Dragon allowed for observing relations between administrators of the organiser's level and local ones. The cooperation required detailed instruction of the latter. The supervisors noted the need for both basic and specialist training as well as complementing ones in the area of cybersecurity. As the studies illus-

trate, in the first stage, Help Desk units – contact points, points of basic technical help should be established within the framework of brigade command battalions, and division command battalions should get support from Service Desk, which should perform incident management, problem management, and change and configuration management tasks. Within the framework of Service Desk operating for the benefit of the division command post, there should be a contact point. In the next stage, depending on the nature and tasks of a military unit, there should be the next point established and responsible for service level management, availability and capacity management. In the author's opinion, establishing new ICT support points in accordance with good practices of the Information Technology Infrastructure Library should, in the long run, give a significant improvement in productivity and efficiency of carrying out the set tasks. ITIL is a set of publications including the best practices of managing IT services. The results of the research in form of observations and also these based on questionnaires and interviews with experts presenting good practices developed in IT departments of governmental institutions and corporations can be used in training soldier candidates and active soldiers of the Armed Forces. ICT systems operated during missions and trainings were provided in accordance with the idea of Federated Mission Networking (Bogdański, 2022, p. 49). The idea of Federated Mission Networking was based on the code of proceedings for IT departments. Information Technology Infrastructure Library made it possible to introduce the following:

— the automation of request handling processes;
— batch processing, which allowed for the execution of certain workloads at a scheduled time;
— planning IT tasks executed in the right time, taking into account the needs concerning process handling, automation of open systems, servers and databases;
— issues concerning the reduction of the number of task executed manually, to enhance process handling;
— proactive monitoring in a service perspective;
— transfer of centrally manager tasks from the first-level Help Desk to the Service Desk and seizing the opportunity for better soldier cooperation.

Sound theoretical knowledge and soldiers' practical skills should be supported by specialist software, also commercial one.

Conclusion

The author of the article conducted his research during the process of training future soldiers and active professional soldiers. He observed practical activities executed during the biggest military practice under the code name of Ana-

konda or Dragon in the Armed Forces of the Republic of Poland. The author performed his observations also during communications and IT army practice under the code name of Aster, which directly preceded the biggest practice managed by the General Command and the Operational Command of the Armed Forces Types. The aim of the article was to determine the impact of good practices in the area of IT on soldier training in the area of cybersecurity. To reach that aim, the author characterized training centres and forms in the Armed Forces in the area of cybersecurity, and defined the impact of a growing number of core and dedicated IT services as well as technical-organisational solutions of command support systems on the training process of communications and IT army soldiers in the area of cybersecurity. The increased use of IT technologies in military operations was a natural evolutionary step. Previously independent, galvanically separated ICT and computer networks, thanks to the IP platform currently converge to one common ICT network. The issue of command process support is gaining importance. The growing number of ICT services and technologies had a substantial impact on the evolution of the training process. As a practical aim, the author of the article wanted to determine the likely direction of change in the way training is provided in terms of implementing and expanding ICT systems and operated services. The studies show that commercial courses and trainings should supplement training forms provided by the Ministry of National Defence.

The main emphasis should be put on good practices in the area of IT. On the basis of his research, the author claims that the influence of this type of courses is crucial for proper management of services in a network-centric environment. The multitude of services enforces systemic actions in the line with schemes. What is more, the author presented the skills that military IT specialists should acquire in order to execute their tasks effectively, characterized good practices used in the system of ICT support, i.e. Help Desk and Service Desk. The cognitive aim was to identify determinants influencing the process of specialized training of communications and IT troops in line units. The research problem was presented by the author in form of the question: What were the differences between the training of IT specialists in civilian and military environments? The performed analysis showed that the training of IT specialists in civilian and military environments differed in particular requirements deriving from the nature of tasks that soldiers were given. In the military environment, security is a priority. On the basis of the research, the author concluded that the training of IT specialists for the needs of the Department of National Defense should encompass specialist subject matters from the area of cybersecurity, defence against cyber attacks and safe information exchange. The author's research also shows that the aforementioned topics were not realised systemically but only within the framework of in-service training. Military IT specialist often have to comply

with strict ethical and legal rules, especially in the context of security, and defence in particular. Military service in strictly regulated by regulations on state secrets. Military IT specialists training often encompasses using highly-specialised tools and technologies that are adjusted to unique military requirements. In the author's opinion, the training should begin by solid foundations in the area of IT, including operational systems, computer networks, databases. IT specialists should be familiarized with the latest technologies and trends in IT. Within the framework of his research, the author conducted the analysis of future soldiers' training in the context of administering IT services used during this training, with the emphasis on the issues concerning cybersecurity. The conclusions drawn from the research dictate that specialized courses led by experts in cybersecurity be organized, beginning with the courses covering the rudiments of cybersecurity such as threat identification, risk analysis, network security. The next stage of the training should cover the subject matter regarding information security and data protection, e. g. specialist courses including the areas such as system penetration, intruder detection, malware analysis, security event management. Practical elements should be introduced, for instance, attack simulation, practical labs and scenarios, so that specialists could gain practical experience.

As for the practical dimension, in the first stage, Help Desk units should be established within the framework of brigade command battalions, and Service Desk should be also established in division command battalions. It should realise tasks in the field of task management, problem management, change and configuration management. Service Desk operating in support of the division command post should be established as a point of contact. In the next stage, depending on the nature of operations and military unit tasks, it would be advisable to consider establishing other units responsible for service level management, availability management, and capacity management.

In the author's opinion, the approach to building ICT support units in accordance with Information Technology Infrastructure Library should in the long run contribute to substantial improvement of capacity and efficiency in realizing basic tasks. As for cybersecurity, the key point for communication and IT troops specialists should be developing skills to effectively use secure leased stationary capacity managed by the Cyberspace Defense Forces Component Command. What is more, it is important to achieve the ability to integrate the stationary and mobile transmission segment by building access points at communication hubs. Developing the ability fostering cooperation of ICT support units in line units with the organizers of ICT systems in operation is key. As the research results based on questionnaires and interviews with experts prove, good practices developed in IT departments of governmental institutions and corporations can be used in training future soldiers and active soldiers in the ArmedForces.

References

Bogdański, A. (2022). Federated Mission Networking w ujęciu narodowych dokumentów doktrynalnych: Aspekt bezpieczeństwa teleinformatycznego. In M. Marczyk, M. Stolarz, & B. Terebiński (Eds.), *Bezpieczeństwo działań w cyberprzestrzeni: wybrane aspekty* (Vol. 2, Techniczne aspekty cyberprzestrzeni, pp. 49–67). Wydawnictwo Akademii Sztuki Wojennej.

Bogdański, A., & Barański, Ł. (2014). Wybrane rozwiązania oraz usługi wdrożone w sieciach teleinformatycznych Wojsk Lądowych. *Bezpieczeństwo i Administracja. Zeszyty Naukowe Wydziału Bezpieczeństwa Narodowego, 1*(1), 167–180.

Bogdański, A., & Zelichowski, A. (2013). Możliwości wykorzystania wojskowych sieci informatycznych w celu prowadzenia badań społecznych w resorcie obrony narodowej. *Obronność – Zeszyty Naukowe Wydziału Zarządzania i Dowodzenia Akademii Obrony Narodowej, 2*(6), 5–19.

Borawska-Kalbarczyk, K. (2024). Edukacja jutra wobec wykorzystania technologii cyfrowych – nowe odpowiedzi na stare pytania. In D. Morańska & P. Oleśniewicz (Eds.), *Edukacja jutra* (pp. 147–159). Oficyna wydawnicza Humanitas.

Ostolski, P. (2020). Kompetencje nauczyciela przedmiotu edukacja obywatelska. Proces kształcenia uczniów wybranych klas mundurowych szkół ponadgimnazjalnych prowadzących przedmiot nauczania edukacja wojskowa. In P. Ostolski & Z. Leśniewski (Eds.), *Proces Kształcenia uczniów wybranych klas mundurowych szkół ponadgimnazjalnych prowadzących przedmiot nauczania edukacja wojskowa* (pp. 183–193). Wydawnictwo Akademii Sztuki Wojennej.

Ostolski, P. (2021). Culture functions for creating security culture. *Security Dimensions, 37*(3), 78–90. https://doi.org/10.5604/01.3001.0015.3294.

Pelc, M. (2012). *Elementy metodologii badań naukowych* (wyd. 1). Wydawnictwo Akademii Obrony Narodowej.

Dowództwo Generalne Rodzajów Sił Zbrojnych. (2017). *Program szkolenia pododdziałów wojsk łączności i informatyki, Dow. Gen. wewn. 79/2017* https://biblioteka.awl.edu.pl/sowacgi.php?KatID=0&typ=record&001=WROC%20WSO17000710.

Minister Obrony Narodowej. (2023, 24 listopada). Rozporządzenie Ministra Obrony Narodowej zmieniające rozporządzenie w sprawie korpusów osobowych, grup osobowych i specjalności wojskowych (*Dz.U. 2023 poz. 2606*). https://sip.lex.pl/akty-prawne/dzu-dziennik-ustaw/zmiana-rozporzadzenia-w-sprawie-korpusow-osobowych-grup-osobowych-i-21901485.

Szkolenie. (n.d.). W *Słownik języka polskiego*. PWN. https://sjp.pwn.pl/slowniki/szkolenie.html.

Sejm Rzeczypospolitej Polskiej. (2022, 11 marca). *Ustawa o obronie Ojczyzny* (*Dz.U. 2024 poz. 248*). https://sip.lex.pl/akty-prawne/dzu-dziennik-ustaw/obrona-ojczyzny-19220069.

ITIL w wersji 4 już dostępny. (n.d.). Compendium. https://www.compendium.pl/info/2023/itil-w-wersji-4-juz-dostepny.

Dobre praktyki w zakresie wojskowego szkolenia z obszaru cyberbezpieczeństwa

Streszczenie

Celem artykułu było określenie wpływu dobrych praktyk w obszarze IT na szkolenie żołnierzy z obszaru cyberbezpieczeństwa. Aby osiągnąć cel autor w artykule scharakteryzował ośrodki i form szkolenia w Siłach Zbrojnych w obszarze cyberbezpieczeństwa oraz określenie wpływu zwiększającej się liczby informatycznych usług podstawowych i dedykowanych, a także rozwiązań techniczno-organizacyjnych systemów wsparcia dowodzenia na proces szkolenia żołnierzy wojsk łączności i informatyki w zakresie cyberbezpieczeństwa. Jako cel praktyczny artykułu autor przyjął określenie prawdopodobnego kierunku zmiany w sposobie szkolenia w aspekcie wdrażania i rozbudowy systemów teleinformatycznych oraz eksploatowanych usług. W artykule autor przedstawił zdolności jakie powinni osiągnąć specjaliści informatycy wojskowi w celu skutecznej realizacji zadań, scharakteryzował dobre praktyki wykorzystywane w systemie wsparcia teleinformatycznego. Celem poznawczym artykułu było zidentyfikowanie determinantów wpływających na procesy szkolenia specjalistycznego wojsk łączności i informatyki w jednostkach liniowych. Problem badawczy autor sprecyzował w postaci pytania: Jakie były różnice pomiędzy szkoleniem specjalistów informatyków w środowisku cywilnym, a wojskowych?

Słowa kluczowe: dobre praktyki, szkolenie, cyberbezpieczeństwo, informatyka, teleinformatyka, bezpieczeństwo informacji, administrowanie, Help Desk, Service Desk.