

PIOTR KOBIELSKI*

Wojskowa Akademia Techniczna, Warszawa, Polska

LAW OF 11 MARCH 2022 ON HOMELAND DEFENSE IMPLICATIONS FOR THE CYBERSECURITY OF POLAND



ABSTRACT: On March 11, 2022, Polish parliament, the Sejm passed the Law on Homeland Defense. The Law replaces 14 other legal acts in the field of military law. The main goal of the Law was to prepare the Polish Armed Forces for the processes of rapid increase in the manpower and technical modernization, also due to the current geopolitical context related to the war in Ukraine. The Law is extensive. Although the improvement of Poland's cybersecurity was not its primary goal, the Law introduces a number of solutions that undoubtedly pursue such a goal. This paper discusses selected issues in the field of cybersecurity included in the Law, and regarding the method of defining the cyberspace, organization and tasks of the Cyberspace Defense Forces, including the so-called proactive protection and active defense, as well as the competence of military authorities to access and manage data.

KEYWORDS: cyberspace, cybersecurity, Cyber Defense Forces, data, law, Poland, Law on Homeland Defense

INTRODUCTION

On 11 March 2022 the lower chamber of Polish parliament, the Sejm, adopted the Law on Homeland Defense (pl. *Ustawa o obronie Ojczyzny*) (the Law)¹. The Law brings a major change in regulatory framework for the Polish Armed Forces (the Armed Forces). This new code-style legislation, combining many legal acts relevant for the military, serves several purposes. It provides organizational and financial basis for anticipated expansion of the Armed Forces, thus

* dr Piotr Kobielski, Military University of Technology, Warszawa, Poland

 <https://orcid.org/0000-0001-5944-3576>,  piotr.kobielski@wat.edu.pl

Copyright (c) 2022 Piotr KOBIELSKI. This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.

¹ Journal of Laws of 2022, Item 655.

adapting to rapidly changing geopolitical situation in the Central and Eastern Europe (CEE). The new legislation is technologically-neutral, open for digital transformation of the Armed Forces. Although the cybersecurity is not the main feature of the Law, the act contains at least three elements relevant for the regulatory framework in this particular regard. These are – the definition of cyberspace, organization of the Cyber Defense Forces, as well as details on access to and transfer of data. All three constitute important elements of the cybersecurity regulatory framework and thus having significant bearing on the cybersecurity of Poland.

LEGISLATIVE PROCESS

Before sharing its intention to table the draft Law the Ministry of National Defense (MOD) must have worked on that initiative for months, if not years. On 12 November 2022, a day after the Independence Day in Poland, the draft Law was formally registered within the legislative pipeline of the Council of Ministers (pl. *Rada Ministrów*)². Until early 2022 different branches of the government had an option to opinion the draft Law. On 22 February 2022 the Council of Ministers approved the draft Law for further works in the parliament. Russian full-scale invasion against Ukraine of 24 February 2022 accelerated the process. On 28 February 2022 the draft Law was registered with the lower house of the parliament – the Sejm. Immediately upon submission to the Sejm the draft Law was sent to the first reading. On 3 March the draft Law passed the first reading. On 11 March – the second. On 11 March, during the third and final reading, the draft law was adopted by the parliament.

Adoption of the draft Law was unique in the sense that out of 460 MPs 450 voted in favor of the act, nobody was against and only 5 MPs abstained. Therefore the draft Law received backing from all political parties. This has happened in usually polarized parliament (there's a common practice that MPs vote against any rational proposal just because it originates from a different political party). The Sejm gave a clear signal to foreign observers, including those in the East, that the national security is outside of political dispute among political groups in Poland.

On 23 March 2022 the Law was officially published in the Journal of Laws (pl. *Dziennik Ustaw*). The Law entered into force on the 30th day from the day of its publication, that is, on

² The Council of Ministers denotes the Polish government.

23 April 2022. It became a new legal framework for organization and financing of the Armed Forces in Poland.

STRUCTURE AND CONTENTS

The Law is composed of divisions and chapters. There are altogether 26 divisions and each division consists of a number of additional chapters. The Law contains altogether 824 provisions. The Law is broad in the scope. Title of each division indicates actual content. Comprehensive list of all titles is the following:

- General provisions (pl. *I. Przepisy ogólne*),
- Defense obligation (pl. *II. Obowiązek obrony*),
- Armed Forces (pl. *III. Siły Zbrojne*),
- National Defense Bodies (pl. *IV. Organy Obrony Narodowej*),
- Programming and financing of the development of the Armed Forces (pl. *V. Programowanie i finansowanie rozwoju Sił Zbrojnych*),
- Military registration and qualification and military inventory (pl. *VI. Rejestracja i kwalifikacja wojskowa oraz ewidencja wojskowa*),
- Recruitment for military service and adjudication of fitness for military service (pl. *VII. Rekrutacja do służby wojskowej oraz orzekanie o zdolności do pełnienia służby wojskowej*),
- Soldiers education (pl. *VIII. Kształcenie żołnierzy*),
- Military service (pl. *IX. Służba wojskowa*),
- Reserve service (pl. *X. Służba w rezerwie*),
- Dogs and horses in the Armed Forces (pl. *XI. Psy i konie w Siłach Zbrojnych*),
- Powers and duties of soldiers (pl. *XII. Uprawnienia i obowiązki służbowe żołnierzy*),
- Military discipline (pl. *XIII. Dyscyplina wojskowa*),
- Salaries of soldiers and other monetary receivables (pl. *XIV. Uposażenie żołnierzy i inne należności pieniężne*),
- Financial liability of soldiers (pl. *XV. Odpowiedzialność majątkowa żołnierzy*),
- Compensation benefits related to military service (pl. *XVI. Świadczenia odszkodowawcze pozostające w związku ze służbą wojskową*),

- Military service in the event of mobilization and in time of war (pl. XVII. *Służba wojskowa w razie ogłoszenia mobilizacji i w czasie wojny*),
- Military service of professional soldiers in the event of mobilization, martial law and in time of war (pl. XVIII. *Służba wojskowa żołnierzy zawodowych w razie ogłoszenia mobilizacji, ogłoszenia stanu wojennego i w czasie wojny*),
- Alternative service (pl. XIX. *Służba zastępcza*),
- Militarization and protection of objects of particular importance to the security or defense of the state (pl. XX. *Militaryzacja i ochrona obiektów szczególnie ważnych dla bezpieczeństwa lub obronności państwa*),
- Service for defense purposes (pl. XXI. *Świadczenia na rzecz obrony*),
- Organizing tasks carried out by entrepreneurs for the Armed Forces (pl. XXII. *Organizowanie zadań realizowanych przez przedsiębiorców na rzecz Sił Zbrojnych*),
- Granting consent to Polish citizens to serve in a foreign army or a foreign military organization (pl. XXIII. *Udzielanie zgody obywatelom polskim na służbę w obcym wojsku lub obcej organizacji wojskowej*),
- Medals (pl. XXIV. *Medale*),
- Penal provisions and provisions on financial penalties (pl. XXV. *Przepisy karne i przepisy o karach pieniężnych*),
- Changes in regulations, transitional, adapting and final provisions (pl. XXVI. *Zmiany w przepisach, przepisy przejściowe, dostosowujące i końcowe*).

The Law repeals altogether 14 acts, including those crucial for the functioning of the Armed Forces. Among those repealed is the Act of 21 November 1967 on the universal obligation to defend the Republic of Poland (pl. *Ustawa o powszechnym obowiązku obrony Ojczyzny*)³, enacted in times when Poland was a communist state and Polish army fully controlled by the Red Army. In order to collect in one place many military provisions, scattered across entire national legislation, as well as to adapt to our times, including the necessity of the army's expansion and modernization, one comprehensive law was more than needed. Previous 14 acts have been replaced by one uniform set of provisions. The Law became a sort of a military code, the law of the first choice for decision-makers, soldiers and military administration.

³ Journal of Laws of 2021, Item 372.

In addition the Law created entirely new system of executive acts – as of the beginning of June 2022 different branches of the government have adopted 31 executive acts. Bearing in mind the short period of time from the adoption of the Law, the number of executive acts already in force is symptomatic, shows how important the Law is for the government.

Although the Law repelled altogether 14 acts, transmitting the majority of their provisions into the new Law, certain subject-matters relevant for the Armed Forces are left outside of its scope. Among the areas covered by separate pieces of legislation are – the martial law and the Supreme Commander of the Armed Forces⁴, the office of the Minister of Defense⁵, the status of foreign armed forces in Poland and Polish Armed Forces abroad⁶ as well as military intelligence and counterintelligence⁷.

CYBERSPACE

As every modern act the Law enshrines a basic catalogue of legal definitions. Among the most important for the cybersecurity of Poland is the one of the cyberspace. The notion of the cyberspace was defined by the reference to already existing legal definition in another legal act. According to Article 2 of the Law⁸ the cyberspace ought to be understood as the one referred to in Article 2(1b) of the Act of 29 August 2002 on martial law and competences of the Supreme Commander of the Armed Forces (the Act). That particular provision, Article 2(1b), stipulates the following:

cyberspace ... is understood as the space for processing and exchanging information created by ICT systems, as defined in Article 3(3) of the Act of 17 February 2005 on the computerization of the activities of entities performing public tasks ..., along with the connections between them and relations with users.⁹

⁴ Journal of Laws of 2017, Item 1932.

⁵ Journal of Laws of 1996, No. 10, Item 56.

⁶ Journal of Laws of 1999, No. 93, Item 1063 and Journal of Laws of 1998, No. 162, Item 1117.

⁷ Journal of Laws of 2006, No. 104, Item 709.

⁸ Journal of Laws of 2022, Item 655. (pl.) *Art. 2 pkt 1. cyberprzestrzeń – należy przez to rozumieć cyberprzestrzeń, o której mowa w art. 2 ust. 1b Ustawy z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej (Dz. U. z 2017 r. poz. 1932).*

⁹ Journal of Laws of 2017, Item 1932; (pl.) *Art. 2 ust. 1b Przez cyberprzestrzeń ... rozumie się przestrzeń przetwarzania i wymiany informacji tworzoną przez systemy teleinformatyczne, określone w art. 3 pkt 3 Ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2017 r. poz. 570), wraz z powiązaniem między nimi oraz relacjami z użytkownikami.*

The aforementioned provision clarifies how to understand the cyberspace – as a space for processing and exchanging information created by the ICT systems. Although the Act does not define the notion of “information” it must be understood as every digital data, either personal or non-personal. The Act contains yet another reference to external piece of legislation. Because the cyberspace is created by “ICT systems” (pl. *systemy teleinformatyczne*) and the Act does not clarify how to understand those systems the reference is made to the Act of 17 February 2005 on the computerization of the activities of entities performing public tasks¹⁰. Article 3 (3) of that particular legislation defines “ICT system” as follows:

[ICT system is] ... a set of cooperating IT devices and software ensuring processing, storage, as well as sending and receiving data via telecommunications networks using a terminal device appropriate for a given type of telecommunications network ...¹¹

Having above in mind one needs to take into account the fact that the cyberspace definition in Polish legislation is complex, meaning – it brings together various elements from different pieces of legislation. The Law defines the cyberspace by the reference to other acts. Such reference method of defining in law, although unclear at the first sight, helps to keep entire legal system more consistent and comprehensive. Thus one can be sure that there is only one definition of the cyberspace in the entire legislation.

The abovementioned reference-made definition of the cyberspace is important yet for another reason. As it was clarified the cyberspace is defined in the Act, a piece of legislation devoted to the martial law. According to the Act the martial law may be introduced in Poland only when national security is exposed to external threat. Such threat may be posed, inter alia, by “activities in the cyberspace” (pl. *działania w cyberprzestrzeni*).

It is therefore unique for the cybersecurity of Poland that both legal concepts, the cyberspace and the martial law, are interlinked in one legal act. And such interlink is made outside the Law, which only refers to that regulation. Moreover, the legislators decided to regulate the cyberspace and the martial law together in one act, as if there were no other manifestations of cyberspace activities, except those during the material law itself. Of course the scope of activities in the cyberspace is much broader than those related to the martial law.

¹⁰ Journal of Laws of 2017, Item 570.

¹¹ (pl.) Art. 3 pkt 3. *system teleinformatyczny – zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniający przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego w rozumieniu przepisów ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. z 2021 r. poz. 576).*

Moreover, there's an activity in the cyberspace that has no bearing on the national security at all (for instance, certain cybercrimes committed in the cyberspace do not pose imminent threat to territorial sovereignty or constitutional order of Poland).

Finally, it needs to be clarified how the cyberspace definition is used in the Law. It appears in the Law on 27 occasions. In general its role is to describe the powers of the Armed Forces, including its cyberspace component. To illustrate, it is stated in the Law that the Armed Forces may “defend and protect the cyberspace” (Article 11(3)), the CDF are suitable for “the full spectrum of activities in the cyberspace” (Article 15 (4)(2)) and the commander of the Cyber Defense Forces is responsible, *inter alia*, for “the security of information in the cyberspace” (Article 23(2)(4)). To conclude, the definition clarifies in what environment the army may execute its competences.

CYBER DEFENSE FORCES

The Law is important for the cybersecurity of Poland also because it creates a legal basis for the Cyberspace Defense Forces (pl. *Wojska Obrony Cyberprzestrzeni*) (CDF) – a new type of the Armed Forces responsible for national security in the cyberspace. For a certain period of time Polish MOD worked on introducing a new type of armed forces into the system. The new component was based on already existing institution supervised by the MOD – the National Cryptology Centre, renamed in 2019 for the National Centre of Cyberspace Security (NCCS) (pl. *Narodowe Centrum Bezpieczeństwa Cyberprzestrzeni*)¹². On 8 February 2022, during a special ceremony at the Military University of Technology, the Minister of National Defense Mariusz Błaszczak handed over a decision appointing general Karol Molenda for the first ever commander of the CDF. From that very moment the new type of the Armed Forces has obtained a command assisted scientifically and technically by the NCCS. From the legal standpoint in February 2022 there has been no such thing as the CDF in Poland yet. This has changed with the adoption of the Law.

The Law formally set up a new type of the Armed Forces in Poland. To the list of already existing land, air, naval, and special forces a new type was added – the CDF. The term CDF appears in the Law on 19 occasions, including in the context of types of the Armed Forces

¹² The Minister of National Defense's Order No. 6 /MOD of 5 March 2019 on changing the name of the state budget unit - National Center for Cryptology to the National Cyberspace Security Center and granting the statute to the National Cyberspace Security Center (Official Journal of the Minister of National Defense of 2019, Item 39)

(Article 15 (4)(2)), their commander (Article 23), as well as various minor changes in already existing laws¹³. Article 15 (4)(2) of the Law stipulates the following:

The Cyberspace Defense Forces, as a specialized component of the Armed Forces, are intended for the implementation of the full spectrum of activities in the cyberspace, in particular in the field of proactive protection and active defense of the cyberspace elements and resources crucial from the point of view of the Armed Forces¹⁴.

As it appears from the abovementioned provision the CDF are a specialized component of the Polish Armed Forces. A “specialized component” (pl. *specjalistyczny komponent*) doesn’t mean they poses less power or they are somehow disadvantaged towards other types of the Armed Forces. Current practice shows that the CDF are paid a special attention by Polish officials, including the MOD, in terms of rapid development and financing of this new type of the Armed Forces. Therefore, the term “component” (pl. *komponent*) doesn’t denote anything particular in legal terms when compared with other types of the Armed Forces.

Furthermore, in the abovementioned description of the CDF there’s a reference made to the area of activity, or rather legal powers of this type of the Armed Forces. The powers are encapsulated in two expressions – “proactive protection” (pl. *proaktywna ochrona*) and “active defense” (pl. *aktywna obrona*) in the cyberspace. Those two expressions are crucial for correct understanding what are the CDF. Its role is not only to passively react to various cyber-attacks but also to actively engage with the enemy to protect certain elements and resources in the cyberspace. It means to engage in defense outside its own networks in order to locate and terminate an attack. This practice is also referred to as the “hack back” – a sort of preemptive attack that can be classified in law as an attack itself and therefore lead to responsibility. There are certain pros and cons of the hack back. On one hand such practice may significantly reduce harm, but on the other, it may lead to unnecessary escalation of hostilities in the cyberspace. General Karol Molenda confirmed that the CDF expected these “proactive” powers to be included in the Law¹⁵.

¹³ See the final provisions in the Law.

¹⁴ (pl.) Art. 14 ust. 4 pkt. 2. *Wojska Obrony Cyberprzestrzeni jako specjalistyczny komponent Sił Zbrojnych są właściwe do realizacji pełnego spektrum działań w cyberprzestrzeni, w szczególności w zakresie proaktywnej ochrony oraz aktywnej obrony elementów i zasobów cyberprzestrzeni kluczowych z punktu widzenia Sił Zbrojnych* (Journal of Laws of 2022, Item 655).

¹⁵ Sz. Palczewski, *Hakerzy Putina w Polsce. Wojsko jest gotowe na operacje rosyjskich specsłużb*, <https://cyberdefence24.pl/armia-i-sluzby/hakerzy-putina-w-polsce-wojsko-jest-gotowe-na-operacje-rosyjskich-specsluzb> (access: 28.07.2022).

International law doctrine has already accepted the policy of the proactive protection and active defense. If there's only a circumstance precluding wrongfulness, like the state of necessity to prevent loss of life, the state is not internationally responsible for engaging in the proactive protection and active defense. Otherwise this state is violating the sovereignty of the target state and thus internationally responsible¹⁶.

Furthermore, Polish legislation is not the first in the world envisaging the proactive protection from ever growing number of various cyberattacks. For instance, in 2017 Tom Graves, a US congressman, submitted to the US Congress a draft-law on the hack back, referred to as the Active Cyber Defense Certainty Act (the ACDC Act)¹⁷. The act waived criminal responsibility in case of the hack-back practices by the victim of cyberattacks. It stipulated that a defender who uses a program, code, or command in response to a cyber intrusion, in order to identify the source of that intrusion, cannot be held criminally responsible under relevant federal laws¹⁸. Although the ACDC Act has never been adopted it can serve as a proof of national practice of the West in relation to the proactive protection and active defense.

In addition to the abovementioned the Law describes the competences of the CDS's commander. Article 23 provides that the commander of the CDS is competent to command military units and their organizational unions. He is supervised by the Minister of National Defense in times of peace and by the Supreme Commander of the Armed Forces in times of an armed conflict. The scope of activities of the commander of the CDS includes, *inter alia*, implementation of the longtime development program of the Armed Forces within conferred competences¹⁹; planning and organizing the mobilization and operational use of the CDS; the construction, maintenance and protection of infrastructure; information protection in the cyberspace; as well as conducting activities and operations in the cyberspace.

DATA

One of the main features of the Law, having a substantive bearing on the cybersecurity of Poland, are data access and data management. In general the Armed Forces gained significant

¹⁶ H. Lahmann, *Hacking Back by States and the Uneasy Place of Necessity within the Rule of Law*, "Heidelberg Journal of International Law" 2020, Vol. 80, p. 457.

¹⁷ R. Chesney, *Hackback Is Back: Assessing the Active Cyber Defense Certainty Act*, <https://www.lawfareblog.com/hackback-back-assessing-active-cyber-defense-certainty-act> (access: 28.07.2022).

¹⁸ Active Cyber Defense Certainty Act, 115th Congress (2017-2018) H.R.4036, <https://www.congress.gov/115/bills/hr4036/BILLS-115hr4036ih.pdf> (access: 28.07.2022).

¹⁹ As adopted by the Council of Ministers and the MOD.

competences related to data, what – in turn – creates certain concerns among specialists and commentators²⁰. Under the Law the army, including the CDF, has a right to process data. This includes both, personal and non-personal data. The competence to process data is of particular concern for all military authorities engaged in the cyberspace in collecting, sorting out and concluding upon substantive stacks of data. Data is of particular interest and attention of the CDF, since many categories of cyberattacks, like for instance the so-called distributed denial of service (DDoS)²¹, are based on big amounts of data.

From the legal standpoint any subject-matter related to national security is excluded from the scope of international and EU legislation. This principle is enshrined, inter alia, in Article 4 (2) of the Treaty on European Union, which stipulates that the EU respects “essential State functions, including ensuring the territorial integrity of the State, maintaining law and order and safeguarding national security”²². The principle is repeated in the EU secondary legislation, including on data. For instance, the General Data Protection Regulation of 2016 stipulates that it “does not apply to the processing of personal data by competent authorities for the purposes of ... safeguarding against and the prevention of threats to public security”²³. In other words competent national authorities have a free hand in adopting such laws on data as necessary to protect national security. The Law is an example of such laws, staying in line with the abovementioned rule.

The Law contains specific provision dedicated to data (Article 10). Its scope of application is general. It provides “military authorities” (pl. *organy wojskowe*) with the competence to “process information” (pl. *przetwarzanie informacji*). It must be understood that the notion of military authorities include the CDF as a specialized formation conducting its operations with the use of data in the cyberspace. Furthermore, to process information means to process both, personal and non-personal data. There are no limitations what sort of data can be utilized. Article 10 (1) of the Law stipulates the following:

²⁰ M. Fraser, *Czy ustawa o obronie Ojczyzny da dostęp do danych obywateli dla wojska poza kontrolą?* <https://cyberdefence24.pl/polityka-i-prawo/czy-ustawa-o-obronie-ojczyzny-da-dostep-do-danych-obywateli-dla-wojska-pozza-kontrola> (access: 28.07.2022).

²¹ DDoS: distributed denial of service.

²² The Official Journal of the EU of 2012, C 326.

²³ Regulation (EE) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (The Official Journal of the EU of 2016, L 119)

Within the scope of their competences, the military authorities process information, including personal data, obtained from data files kept by other services, state institutions and public authorities. The processing of information, including personal data, by military authorities may be classified, without the consent and knowledge of the data subject ...²⁴

The military authorities may obtain data from almost all public institutions which are thus legally obliged to respond to the request for data sharing:

Services, state institutions and public authorities are obliged to make information, including personal data, available to the military authorities free of charge. In particular, military authorities are entitled to obtain information, including personal data collected in data files or registers administered by these services, state institutions and public authorities²⁵

The abovementioned provisions related to data management by the military authorities, including by the CDF, seems natural and obvious for security experts, as they secure the competence of the Armed Forces to dive deep into any data pool in order to collect information crucial for the national security.

This security-oriented competence is crucial for the cybersecurity of Poland. If we assume that modern battlefield is replaced by the cyberspace and tangible weaponry by data²⁶, then no access to big stacks of data undermines the very sense of the existence of the CDF. They need data for the proactive protection and active defense in their daily routine²⁷. Moreover, the cybersecurity forces are not the only ones to deal with data issues. Also other types of the Armed Forces need to adapt to digital transformation, including data management²⁸.

²⁴ (pl.) Art. 10. ust. 1. *Ustawy Organy wojskowe w zakresie swojej właściwości przetwarzają informacje, w tym dane osobowe, uzyskane ze zbiorów danych prowadzonych przez inne służby, instytucje państwowe oraz organy władzy publicznej. Przetwarzanie informacji, w tym danych osobowych, przez organy wojskowe może mieć charakter niejawnny, odbywać się bez zgody i wiedzy osoby, której dane dotyczą. Służby, instytucje państwowe oraz organy władzy publicznej są obowiązane do nieodpłatnego udostępnienia organom wojskowym informacji, w tym danych osobowych. W szczególności organy wojskowe są uprawnione do uzyskiwania informacji, w tym danych osobowych gromadzonych w administrowanych przez te służby, instytucje państwowe oraz organy władzy publicznej zbiorach danych lub rejestrach* (Journal of Laws of 2022, Item 655).

²⁵ Journal of Laws of 2022, Item 655.

²⁶ Col. B. Graboritz, Lt. Col. J. Morford, Maj. K. Truax, *Why the Law of Armed Conflict (LOAC) Must Be Expanded to Cover Vital Civilian Data*, "The Cyber Defense Review" Fall 2020, Vol. 5, No. 3, pp. 121-132.

²⁷ For the national security context see for instance: B. Smith, C. Browne, *Tool and Weapons*, Hodders & Stoughton, London, 2021, p. 26.

²⁸ In the US, for instance, the Marine Corps moves to formalize its doctrine on the information environment. See: M. Pomerleau, *Marine Corps to release new doctrine on Information*, <https://www.fedscoop.com/marine-corps-to-release-new-doctrine-on-information/> (access: 28.07.2022). For more information on Big Data in Polish Armed Forces see: <https://wcy.wat.edu.pl/pl/news/seminarium-naukowe-big-data-w-silach-zbrojnych-rp> and <https://nup.wp.mil.pl/pl/articles6-aktualnosci/seminarium-naukowe-nt-technologie-big-data/>, (access: 28.07.2022).

Almost immediately after the adoption of the Law fundamental rights activists highlighted the risk of uncontrolled and unlimited access to data by the Armed Forces. Although the commentators understood the rationale behind Article 10 (see above) public discussion focused on potential safeguards to be introduced into the Law in future, like, for instance, setting up a special governmental plenipotentiary supervising military access to data²⁹. Should the army be controlled or supervised in respect of data handling is an open question. Without any such safeguard in place, as it was argued, the army may infringe fundamental rights of Polish citizens, such as the respect for privacy and family life. Moreover, bearing in mind the principle of proportionality, it is rather inconvincible that the Armed Forces actually need all the data stored, for instance, by pension or healthcare public agencies³⁰. The time will show whether any changes to the Law are necessary.

CONCLUSIONS

When the Law was passed few may have expected that it can affect the cybersecurity of Poland in any significant manner. Its prime purpose was to provide organizational and financial basis for anticipated expansion of the Armed Forces, taking into account the war in Ukraine and rapidly changing geopolitical situation of the CEE. Yet, thorough analysis of the Law leads to conclusion on inevitable digital transformation of the Armed Forces, and more generally – its impact on the cybersecurity of Poland. As presented in this paper the Law contains at least three elements relevant for the regulatory framework in this regard. These are – the definition of the cyberspace, the organization of the CDF, as well as an access to and transfer of data crucial for the proactive protection and active defense in the cyberspace. All three elements constitute important feature of the cybersecurity regulatory framework and thus have significant bearing on the cybersecurity of Poland. The practice under the Law will prove to what extent it contributes to the overall cybersecurity of the state and its agencies, including the Armed Forces.

²⁹ This type of control of data management is used in anticorruption proceedings – see Article 22 of the Act of 9 June 2006 on the Central Anti-Corruption Bureau (Journal of Laws of 2006, No. 104, Item 708).

³⁰ M. Fraser, *Czy ...*, *op. cit.*

REFERENCES LIST

LITERATURE

Smith B. , Browne C., *Tool and Weapons*, Hodders & Stoughton, London, 2021

Grabowitz B. , Morford J., Truax K., *Why the Law of Armed Conflict (LOAC) Must Be Expanded to Cover Vital Civilian Data*, "The Cyber Defense Review" Fall 2020, Vol. 5, No. 3

Lahmann H., *Hacking Back by States and the Uneasy Place of Necessity within the Rule of Law*, "Heidelberg Journal of International Law" 2020, Vol. 80

Chesney R., *Hackback Is Back: Assessing the Active Cyber Defense Certainty Act*,

<https://www.lawfareblog.com/hackback-back-assessing-active-cyber-defense-certainty-act>

Fraser M., *Czy ustawa o obronie Ojczyzny da dostęp do danych obywateli dla wojska poza kontrolą?*

<https://cyberdefence24.pl/polityka-i-prawo/czy-ustawa-o-obronie-ojczyzny-da-dostep-do-danych-obywateli-dla-wojska-pozza-kontrola>

Palczewski Sz., *Hakerzy Putina w Polsce. Wojsko jest gotowe na operacje rosyjskich specsi*,

<https://cyberdefence24.pl/armia-i-sluzby/hakerzy-putina-w-polsce-wojsko-jest-gotowe-na-operacje-rosyjskich-specsluzb>

Pomerleau M., *Marine Corps to release new doctrine on Information*, <https://www.fedscoop.com/marine-corps-to-release-new-doctrine-on-information/>

SOURCES

Consolidated Version of the Treaty on European Union (The Official Journal of the EU of 2012, C 326)

Regulation (EE) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (The Official Journal of the EU of 2016, L 119)

Law of 11 March 2022 on Homeland defense (Journal of Laws of 2022, Item 655)

Act of 17 February 2005 on the computerization of the activities of entities performing public tasks (Journal of Laws of 2017, Item 570)

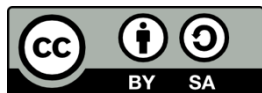
Act of 29 August 2002 on martial law and competences of the Supreme Commander of the Armed Forces (Journal of Laws of 2017, Item 1932)

Act of 21 November 1967 on the universal obligation to defend the Republic of Poland (Journal of Laws of 2021, Item 372)

Active Cyber Defense Certainty Act, 115th Congress (2017-2018) H.R.4036



Copyright (c) 2022 Piotr KOBIELSKI.



This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.