Piotr Szreniawski[*]

The State as a Learning Organization and Cybersecurity

Abstract

In a contemporary state, cybersecurity is becoming an increasingly important issue. In order for a state to adequately respond to changing threats, it must be a learning organization. Learning about cybersecurity should include specialist knowledge, but also knowledge about cybersecurity shaping the behaviours of the general public and policy makers. Legal regulations are an important instrument of shaping cybersecurity in a learning state.

Key words: cybersecurity, state, learning

[*] Assoc. Prof. Piotr Szreniawski, PhD, Katedra Prawa Administracyjnego i Nauki o Administracji, Instytut Nauk Prawnych, Uniwersytet Marii Curie-Skłodowskiej w Lublinie, e-mail: piotr.szreniawski@mail.umcs.pl.

If we look at the state as at a situation in which there is power, the learning process will be based on changing the situations. Learning is usually defined as a permanent change of behaviour, therefore, for state learning to occur, the transformation of a series of situations must show a certain continuity or regularity. The assumption of the existence and of observation of regularities is similarity, just as similarity is the primary principle of the existence of law in general. Similarity is something other than difference or no similarity. In this context, we can notice the connection between the learning processes and changes in the behaviour of authorities, or changes in the relations between authorities and individuals subject to the state power. By learning, the state changes the norms of behaviour, including, above all, the legal norms, but also the actual behaviour of those in power. Cybersecurity is associated with constant change. The state participates in the cybersecurity race by competing with other states or organizations threatening cybersecurity. This process of change can be seen as learning.

Knowledge is one of the resources essential in the competitive struggle, both in terms of competition on the market between private entities and in the area of the public sphere, including in relation to competition between states. The state is a specific type of organization related to power, covering the territory, and permanently influencing the population. Analyzes of state learning should be undertaken while taking into account issues such as organizational learning, learning organizations and knowledge management. Public administration deals with a number of threats in the field of cybersecurity, not only solving problems concerning citizens or entrepreneurs, but being itself the target of various – more or less professionally prepared – attacks. The human factor in taking care of security is one of the extremely important issues[1], so not only antivirus programs or the readiness of infrastructure to attack is important here, but also the caution of officials and their training[2].

Lawyers operating in public administration are also exposed to cyber attacks, including attacks related to attempts of obtaining information by unauthorized persons. The use of computers and smartphones in the work of a lawyer is common today, and the processing of personal data or confidential

[1] T.T. Nguyen, V.J. Reddi, *Deep Reinforcement Learning for Cyber Security*, „IEEE Transactions on Neural Networks and Learning Systems" (Early Access) 2021, s. 3.

[2] W. Dziomdziora, *Jak przygotować urząd na cyberatak – aspekty organizacyjno-prawne* [in:] *Cyberbezpieczeństwo w jednostkach samorządu terytorialnego*, ed. D. Myrcha, Warszawa 2018, s. 15.

data, including those relating to the office, but also administration clients, should be associated with the observance of security rules. Activities in this area are often undertaken by local governments of legal professions, including the self government of legal advisers – which is of great importance for public administration due to the employment of legal advisers in public administration[3].

The personification of organizations, including state organizations, may be associated with assigning organizations such features as intelligence, memory or emotions[4]. Intelligent state behaviour includes rules-compliant actions and opportunities, but also environmental adaptation related to learning processes. Obtaining the synergy effect within the state apparatus also requires learning how to cooperate with other persons and entities operating within the state apparatus. At the micro level, decisive for the synergy effect is the appropriate selection of people participating in the work of the organizational unit of the office, including appropriate communication. In the field of cybersecurity, communication matters are of key importance, such as the need to exchange information or develop an appropriate control culture related to openness and striving to ensure high quality, and not to punish or hide imperfections. Learning by the state administration, both at the micro, meso and macro level, requires balancing trust and readiness to respond to errors, but also appropriate assessment of policy issues, including organizational policy.

The political sphere, which can be understood as related to the achievement of goals, is also connected with the rivalry of factions or individuals. Friendships and dislikes, and at a higher level, alliances and conflicts between organizations, can not only fuel action and increase alertness, but also reduce agility and prevent the entire organization from achieving its goals. A state in which public administration is internally conflicted cannot be sure whether emerging cyber attacks should be disclosed – due to the risk of information about cyber attacks being used by political competition, nor can it even be sure whether they are not the work of rival groups. On the other hand, the complete absence of disagreements limits ingenuity and discourages authenticity, forcing individuals and groups to conform to the views that are deemed to be the only right one. Hence, a great role – also in the field of cybersecurity – is played by internal and external control, including judicial or media control.

[3] W. Dziomdziora, *Cyberbezpieczeństwo w samorządzie terytorialnym: praktyczny przewodnik*, Warszawa 2021, p. 109.

[4] J.M. Moczydłowska, *Organizacja inteligentna generacyjnie*, Warszawa 2018, p. 77.

Long-term development programs in the field of talent management may include organizing and appropriate selection of training, or assessing the possibility of using employees' talents at selected positions in the organization[5].

However, from the perspective of the state, talent management covers the entire education system, both at the level of counseling and managing the career of individuals and groups of people, as well as at the level of shaping the education model, including cybersecurity education. The education system must include in this respect both specialist knowledge, combining security issues and broadly understood computer science, but also the transfer of knowledge in the field of cybersecurity to the general public[6].

The state, as a learning organization, relies on using the talents of its inhabitants, which talents are wasted when security issues make it impossible to deal with substantive matters related to the work of individual people. Moreover, attention should be paid to the cybersecurity aspects of the functioning of education. Not only false alarms and threats sent via e-mail, but also data leaks or disrupting the activities of schools – including during exams – in the field of cybersecurity, can reduce the quality of education. On the other hand, the visibility of cybersecurity problems may sensitize both the school administration and students to the importance of the issue of appropriate behaviour in the face of threats. Continuous training, sharing information on threats and counteracting threats must be part of today's primary, secondary and higher education. Of course, undertaking research must also take into account cybersecurity issues.

The issue of state learning should be seen in an international context. Cybersecurity threats occur in many countries, and experience in counteracting threats can also be gained from foreign sources. Moreover, learning about threats originating from abroad is clearly an example that combines the issues of state learning and cybersecurity. Information warfare is a constant element of the functioning of the state in the international arena. The infosphere is a combat environment, and the availability of reliable information is an important good that enables the rational operation of the state and society[7].

[5] J. Tabor-Błażewicz, *Zarządzanie talentami w przedsiębiorstwie kreatywnym* [in:] *Organizacja kreatywna – teoria i praktyka*, eds. P. Wachowiak, S. Gregorczyk, Warszawa 2018, p. 135–136.

[6] B. Czerniachowicz, *Koncepcje organizacji uczącej się i inteligentnej w jednostce samorządu terytorialnego*, „Ekonomiczne Problemy Usług" 2011, no. 77, p. 70.

[7] T.R. Aleksandrowicz, *Zagrożenia dla bezpieczeństwa informacyjnego państwa w ujęciu systemowym. Budowanie zdolności defensywnych i ofensywnych w infosferze*, Warszawa 2021, p. 32–33.

It is essential for political leaders to make good decisions, to embed them in reality, not to distance themselves from those willing to criticize wrongdoing. It should be noted that even people perceived as lonely political leaders must cooperate with their immediate environment, otherwise the risk of making wrong strategic decisions increases. When co-creating a strategy, it is crucial to take into account many different factors that are important for the results of long-term activities. Usually the security perspective is present in all activities of a strategic nature[8]. It should be noted here that also communication within the framework of close leadership – be it political or military – nowadays is associated with the constant existence of threats in the field of information flow and the use of technology.

One of the ways in which a public institution focuses on learning is to prepare selected employees to take on the role of internal trainers[9]. Such practices may be formalized or may be part of management processes. In each case, they should include the creation of training programs, conducting these trainings and their evaluation, but also participation in communication between employees and staff deciding on the direction of the institution's development. In public administration – and in a broader sense, in the state apparatus – elements known from the learning of business organizations, such as coaching or individual training trips, can also be used to some extent. It should be noted that an inseparable element of the functioning of public administration is its link with political factors, which often focus on shaping the image and selection of personnel, rather than on education. In this context, an indispensable, even obvious element of a coherent learning process of the state is not only to educate staff during their work in administration, but above all to create a solid basis for acquiring practical knowledge by broadening horizons and teaching theoretical foundations during education at the level of primary and secondary schools. secondary and higher education. It is worth noting that apart from the knowledge and skills useful for work in the state apparatus, including office work, it is extremely important to develop the habits of good time organization, accuracy and effectiveness, as well as learning habits. Learning during studies, as well as during the earlier stages of education, should be considered broadly, so issues such as activity in student and student organizations, or shaping social attitudes and healthy habits during sports

[8] P.M. Senge i in., *Piąta dyscyplina – materiały dla praktyka*, Kraków 2002, p. 505 et seg.

[9] M. Capiga, *Trenerzy wewnętrzni* [in:] *Jak wzmacniać organizacyjne uczenie się w administracji rządowej*, eds. B. Ledzion, K. Olejniczak, J. Rok, Warszawa 2014, p. 203.

activities or developing creativity during artistic activities are important here. The self-knowledge of individual administration employees enables them to use their talents, but the ability to compose teams appropriately is also necessary to build the organization of an effective learning state.

In a broader context, an element of state learning is also learning history. Building identity, caring for the continuity of the state or identifying with features related to tradition should be adapted to contemporary phenomena, for example related to cybersecurity. Information activities on the internet, as well as the use of available tools, do not undermine the achievements of generations related to caring for the common good or not disclosing valuable information to unauthorized persons. The creation of new knowledge by the state apparatus concerns, inter alia, getting to know the state apparatus itself, operating in new circumstances[10]. Of course, also specialized public entities, related to research development, information processing or intelligence, are also closely related to the learning processes of the state.

An element of organizational learning is changes in the organizational culture. The state must react particularly to issues related to security, including shaping its organizational culture. The preparation of appropriate training, case studies as well as communication using feedback is useful for the appropriate transformation of the organizational culture. Analyzes of the existing organizational culture in public administration and the state apparatus as a whole should be carried out reliably, as far as possible without adopting party criteria, and focusing more on the national perspective, taking into account the criteria of efficiency and security[11].

Additionally, for the appropriate shaping of organizational culture in the entire state apparatus, it is necessary to coordinate activities – not only in the field of training, but e.g. in the field of responding to incidents related to cybersecurity[12]. The law is an extremely important element coordinating not only the structure, forms and scope of the state's activity, but also influencing the organizational culture. Law, being an instrument that comprehensively

[10] A. Domaradzka et al., *Co powinniśmy mierzyć, czyli elementy mechanizmu uczenia się* [w:] *Jak diagnozować mechanizm uczenia się w organizacjach rządowych*, eds. K. Olejniczak, P. Śliwowski, Warszawa 2014, p. 20.

[11] B. Czerniachowicz, *Wybrane problemy budowania organizacji uczącej się* [in:] *Organizacja inteligentna – perspektywa zasobów ludzkich*, eds. C. Suszyński, G. Leśniak-Łebkowska, Warszawa 2016, p. 24.

[12] C. Banasiński, *Prawne i pozaprawne źródła wymagań dla systemów cyberbezpieczeństwa* [in:] *Cyberbezpieczeństwo*, eds. C. Banasiński, M. Rojszczak, Warszawa 2020, p. 19.

influences the modern state, is an element of self-regulation, including self-limitation of this state. One of the dimensions of limiting the freedom of action of administrative entities is the security dimension, which also includes cybersecurity. In this context, learning by the state also consists in getting to know the content of new regulations, but also in standardizing the jurisprudence or in taking into account the realities – even economic – in which public administration operates, dealing with specific matters. Of course, it is also necessary to take into account the security dimension when assessing the realities of operations, including, for example, learning about the methods of operation of terrorist organizations in the network[13].

For cybersecurity in the context of perceiving the state as a learning organization, it is essential to learn not only selected parts of the state organization that specialize in counteracting threats in the field of cybersecurity, although it is as important as education in the field of cybersecurity of broad social groups. However, education in the field of cybersecurity of people making decisions in the state, i.e. primarily political leaders, is of great importance. Permanent implantation of an element of cyber security in the state organization is an important task of shaping the political elite and public discourse in general. The role of cybersecurity specialists is therefore not limited to improving their own knowledge, but also includes tasks in the field of educating people working in the state apparatus, including people occupying the highest state positions[14].

It should be noted that the growing importance of cybersecurity in the modern world should be combined with the perception of this element during legislative work. Both the creation of norms of systemic and procedural law, as well as taking into account the cybersecurity dimension in substantive law are important both in terms of the organization of uniformed services and civil administration. For the efficiency of operation, as well as for the effectiveness of public administration, it is necessary to constantly follow, and even anticipate, trends in emerging threats[15].

[13] J. Absi, *Cyberbezpieczeństwo we współczesnych konfliktach na Bliskim Wschodzie*, Poznań 2019, p. 33.

[14] M. Musser, A. Garriott, *Machine Learning and Cybersecurity*, Georgetown 2021, p. 36.

[15] K. Olejniczak, J. Rok, A. Płoszaj, *Organizacyjne uczenie się i zarządzanie wiedzą – przegląd koncepcji* [in:] *Organizacje uczące się. Model dla administracji publicznej*, ed. K. Olejniczak, Warszawa 2012, s. 102.

Bibliography

Absi J., *Cyberbezpieczeństwo we współczesnych konfliktach na Bliskim Wschodzie*, Poznań 2019.

Aleksandrowicz T.R., *Zagrożenia dla bezpieczeństwa informacyjnego państwa w ujęciu systemowym – budowanie zdolności defensywnych i ofensywnych w infosferze*, Warszawa 2021.

Banasiński C., *Prawne i pozaprawne źródła wymagań dla systemów cyberbezpieczeństwa* [in:] *Cyberbezpieczeństwo*, eds. C. Banasiński, M. Rojszczak, Warszawa 2020.

Capiga M., *Trenerzy wewnętrzni* [in:] *Jak wzmacniać organizacyjne uczenie się w administracji rządowej*, eds. B. Ledzion, K. Olejniczak, J. Rok, Warszawa 2014.

Czerniachowicz B., *Koncepcje organizacji uczącej się i inteligentnej w jednostce samorządu terytorialnego*, „Ekonomiczne Problemy Usług" 2011, no. 77.

Czerniachowicz B., *Wybrane problemy budowania organizacji uczącej się* [in:] *Organizacja inteligentna – perspektywa zasobów ludzkich*, eds. C. Suszyński, G. Leśniak-Łebkowska, Warszawa 2016.

Domaradzka A. et al., *Co powinniśmy mierzyć, czyli elementy mechanizmu uczenia się* [in:] *Jak diagnozować mechanizm uczenia się w organizacjach rządowych*, eds. K. Olejniczak, P. Śliwowski, Warszawa 2014.

Dziomdziora W., *Cyberbezpieczeństwo w samorządzie terytorialnym: praktyczny przewodnik*, Warszawa 2021.

Dziomdziora W., *Jak przygotować urząd na cyberatak – aspekty organizacyjno-prawne* [in:] *Cyberbezpieczeństwo w jednostkach samorządu terytorialnego*, eds. D. Myrcha, Warszawa 2018.

Moczydłowska J.M., *Organizacja inteligentna generacyjnie*, Warszawa 2018.

Musser M., Garriott A., *Machine Learning and Cybersecurity*, Georgetown 2021.

Nguyen T.T., Reddi V.J., *Deep Reinforcement Learning for Cyber Security*, „IEEE Transactions on Neural Networks and Learning Systems" (Early Access) 2021.

Olejniczak K., Rok J., Płoszaj A., *Organizacyjne uczenie się i zarządzanie wiedzą – przegląd koncepcji* [in:] *Organizacje uczące się. Model dla administracji publicznej*, ed. K. Olejniczak, Warszawa 2012.

Senge P.M. et al., *Piąta dyscyplina – materiały dla praktyka*, Kraków 2002.

Tabor-Błażewicz J., *Zarządzanie talentami w przedsiębiorstwie kreatywnym* [in:] *Organizacja kreatywna – teoria i praktyka*, eds. P. Wachowiak, S. Gregorczyk, Warszawa 2018.

Państwo jako organizacja ucząca się a cyberbezpieczeństwo

Streszczenie

We współczesnym państwie cyberbezpieczeństwo staje się coraz ważniejszym zagadnieniem. Żeby państwo odpowiednio reagowało na zmieniające się zagrożenia, musi być organizacją uczącą się. Uczenie się cyberbezpieczeństwa powinno obejmować wiedzę specjalistyczną, a także wiedzę o cyberbezpieczeństwie kształtującą zachowania ogółu społeczeństwa i decydentów politycznych. Ważnym instrumentem kształtowania cyberbezpieczeństwa w państwie uczącym się są przepisy prawa.

Słowa kluczowe: cyberbezpieczeństwo, państwo, uczenie się