

MICHAŁ JUREK\*

Wojskowa Akademia Techniczna, Warszawa, Polska

## THE IMPACT OF CITIZENS' CYBERSECURITY ON THE STATE SECURITY LEVEL

**ABSTRACT:** In the heavily computerized world based on networks (e.g., social or computer networks) and IT tools, the level of security of citizens in cyberspace will play an increasingly important role in ensuring state security. In fact, cyber threats may affect not only individual units, but also entire systems composed of diverse components. The purpose of this paper is to indicate what effect the actions taken by citizens in cyberspace have on state security. Therefore, it is necessary to find answers to the following questions: Can citizens significantly affect the level of state security? How can the actions taken by citizens in cyberspace influence the formation of the level of state security? The author used the following research methods in his research: system approach, comparison, inference, analogy, abstraction and generalization.



**KEYWORDS:** cyberspace, cyber threats, citizen, security, state and citizen security.

### INTRODUCTION

In the time of widespread digitalization, i.e. the transformation of all elements of reality into data for appropriate processing (aggregation and algorithmization), actions taken in cyberspace by individuals or entities (citizens, systems) will gain in relevance<sup>1</sup>. This is because

---

\* Michał Jurek, Military University of Technology, Warsaw, Poland

 <https://orcid.org/0000-0003-0949-7458>,  [michal.jurek@wat.edu.pl](mailto:michal.jurek@wat.edu.pl)

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

<sup>1</sup> Vide Ł. Iwasiński, *Spółeczne zagrożenia danetyzacji rzeczywistości*, [in:] *Nauka o informacji w okresie zmian. Informatologia i humanistyka cyfrowa*, red. B. Sosińska-Kalata, Wydawnictwo Naukowe i Edukacyjne SBP, Warszawa 2016.

they will lead to the creation of artifacts (e.g. data, information, legal effects, etc.), the generation of which will result in a change in the state of the original reality. These changes should be monitored in order to make visible possible threats that may affect a given unit or a given system (network).

The monitoring system itself should be adequately standardized and supervised. Standardization will enable the unification of rules that, after a certain generalization (standardization), can be implemented in entities regardless of the sector (private, public) they originate from<sup>2</sup>. Such rules, once simplified, will also find application in monitoring activities undertaken in cyberspace by individual entities. Unification of monitoring rules is going to translate into stabilization of the operation of entities or units, for example, by being able to identify and reduce redundant activities or undesirable actions<sup>3</sup>.

Supervision of the monitoring system should be based on three columns:

1. multidimensionality,
2. verifiability,
3. quantifiability and evaluability<sup>4</sup>.

The multidimensionality will allow for a detailed examination of the different-level relationships linking the actions taken within the above system and the effects they generate<sup>5</sup>. This will enable measurement of the processes taking place in it and their evaluation, for example, through the prism of quality, efficiency or usefulness. Quantification and evaluation will translate into the possibility of verification of the obtained results by third (independent) entities or units. It will result in an increase in the quality level of the monitoring system itself through the possibility of verification of the correctness and authenticity of the obtained results by the supervising entity and the possibility of pointing out originally unidentified problems.

When analyzing the above assumptions, it can be noted that the actions taken in cyberspace can affect not only individuals (citizens), but also entities, such as states or organizations. They can also generate effects of not only local or regional, but also global nature. Therefore, it is necessary to indicate what capabilities a state has to counter threats from cyberspace, and how

---

<sup>2</sup> K. Rostek, K. Gołuch-Trojanek, *Standaryzacja procesów i jej rola w procesie wdrażania zintegrowanych systemów informatycznych w instytucjach publicznych: (na przykładzie uczelni publicznej)*, „Autobusy: technika, eksploatacja, systemy transportowe” 2017, vol. 18, no. 9, p. 56-57.

<sup>3</sup> Ibidem.

<sup>4</sup> Vide Strona internetowa NIK, <https://www.nik.gov.pl/>, „Standardy Kontroli NIK” (accessed: 21.07.2022).

<sup>5</sup> The different levels of relationships should be understood as connections between the subsystems (e.g. information, human resources) that make up the monitoring system.

the level of situational awareness of cyber threats among its citizens is developing. Doing so will allow us to examine how the level of citizens' cyber security affects the security of the state.

## **STATE VS. CYBERSPACE**

Since the beginning of its existence (as a general entity), the state has been an organizational form of societies with a high degree of hierarchy<sup>6</sup>. The formation of this type of organization was made possible by people joining together in groups to meet both material and spiritual needs<sup>7</sup>. Over the years, the state has evolved in terms of its role in human life. This is because initially it only served to meet the basic needs of individuals. Only in later periods did its role increase and the state became a full-fledged guarantor of citizens' security and regulator of their functioning<sup>8</sup>.

Technical and technological developments have played a major role in this transformation, which has enabled the creation of new tools and ways of communicating<sup>9</sup>. The related phenomenon of ever-increasing digitization and digitalization, as well as the ever-increasing role of information and communication technologies, has resulted in the transfer of core areas of state activity to cyberspace<sup>10</sup>. This is because the computerization of the state allows citizens to use its resources without having physical versions of them (e.g., documents). Remote access to resources carries the risk of threats that can cause significant material as well as intangible losses. These include, for example: blocking access to services/resources, unauthorized change of data, data theft, identity theft, propagation of false information. It is noticeable that these threats are linked directly to the data and information that are processed in the information systems used by the state. The materialization of any of the above risks can result in the loss of financial and human resources, the trust of citizens and, in extreme cases, even the interruption of the entity's business continuity. The continuity of operations, including the informational one, will be keyly influenced by the level of citizens' trust in the state. After all, in the event of its reduction or complete loss, there may even be a disintegration of this form of social organization.

---

<sup>6</sup> D. Dudek, Z. Husak, G. Kowalski, W. Lis, *Konstytucyjny system organów państwa*, Warszawa 2012, p. 1.

<sup>7</sup> J. Krukowski, *Wstęp do nauki o państwie i prawie*, Lublin 2004, p. 14.

<sup>8</sup> D. Dudek, Z. Husak, G. Kowalski, W. Lis, *Konstytucyjny system organów państwa*, op. cit., p. 2-5.

<sup>9</sup> M. Mindur, *Wpływ postępu technicznego i technologicznego oraz wydarzeń politycznych na rozwój gospodarki globalnej*, „Logistyka” 2012, vol. 3, p. 1623.

<sup>10</sup> Główny Urząd Statystyczny, <https://stat.gov.pl/>, „Społeczeństwo informacyjne w Polsce w 2021 r.” (accessed: 21.07.2022).

When analyzing the state's activities in cyberspace, special attention should be paid to its genesis. After all, cyberspace is a creation of man, which is used for the exchange of information<sup>11</sup>. The most important differences between the aforementioned environments and the land, sea, air and space environments are shown in Table 1.

Table 1

Comparison of land, sea, air and space environments with cyberspace

Land, sea, air, space environment	Cyberspace
Natural	Artificial
Formation possibilities are limited	Users have full control over its formation
Territorially limited	No territorial limitations

Source: own study based on M. Marczyk, *Cyberprzestrzeń jako nowy wymiar aktywności człowieka (Cyberspace as a new dimension of human activity) – conceptual analysis*, „Przegląd teleinformatyczny” (ICT Review). 2012, vol. 6, no. 1-2, pp. 60.

Analyzing the characteristics of the planes shown in Table 1, it can be seen that cyberspace is an aterritorial creation. This is because its boundaries cannot be defined explicitly. This results in the ability to connect to the network anywhere at any time<sup>12</sup>. The only constraints in the aforementioned case will be the technical capacity to connect to the network and the bandwidth itself<sup>13</sup>.

Analyzing the above elements, it can be seen that a key factor for the state to undertake effective cyberspace activities, as well as its security, is the proper safeguarding of processed data and information. The implementation of appropriate tools and organizational and legal solutions in this regard will normalize the level of information security. We can define information security as the level of a given entity's confidence in the quality and availability of the information it obtains and transposes<sup>14</sup>.

<sup>11</sup> M. Marczyk, *Cyberprzestrzeń jako nowy wymiar aktywności człowieka – analiza pojęciowa obszaru*, „Przegląd teleinformatyczny” 2012, vol. 6, no. 1-2, p. 59.

<sup>12</sup> Ibidem, p. 61.

<sup>13</sup> Ibidem.

<sup>14</sup> K. Liderman, *Bezpieczeństwo informacyjne. Nowe wyzwania*, Warszawa 2017, p. 18.

However, to be able to fully illustrate the phenomenon of information security, it is necessary to distinguish the relevant attributes of information and its security. They can be divided into two categories, which are shown in Table 2.

Table 2

Information attribute categories

Physical factors	Technical factors
Content, form and information user	Organizational and technical criteria for information processing

Source: Own study based on K. Liderman, *Bezpieczeństwo informacyjne. Nowe wyzwania (Information Security. New challenges)*, Warszawa 2017, pp. 16-17.

Therefore, it can be concluded that for information to be of sufficient quality it must have the following characteristics:

- Relevance - the importance of the information to the recipient,
- Accuracy - the precise way of presenting the content of the information,
- Timeliness - change of information occurs without unnecessary delay,
- Completeness - information is available in a degree and quantity that matches the user's requirements,
- Consistency - non-contradiction of fragments of information,
- Appropriateness of form - the way information is presented to reduce misunderstanding,
- Credibility - elements that ensure the reliability of the information provided<sup>15</sup>.

Information that does not meet even one of the aforementioned characteristics will negatively affect the formation of information security. This may translate into a reduced ability to respond to information security incidents. To talk about qualitatively appropriate information in terms of the possibility of its technical processing it is necessary to distinguish the following criteria:

- Secrecy (confidentiality) - the level of protection of information from unauthorized access,
- Integrity - the absence of unauthorized changes,

---

<sup>15</sup> Ibidem, p. 16.

- Availability - level of access to information for processes and applications,
- Accountability - the ability to identify the owner of the information and the systems they use to propagate it,
- Incontestability - the ability to attribute the author of the information,
- Authenticity - the ability to unambiguously identify the entity sending the data<sup>16</sup>.

From the above information quality criteria, it is possible to extract a triad of information security attributes, the disruption of which can prevent total access to information. This will translate into a complete disruption of the information continuity of state operations. This triad consists of the following information attributes: confidentiality, integrity and availability<sup>17</sup>. Without ensuring an appropriate level of confidentiality, unauthorized parties will be able to see the information being sent. This may pose a risk of acquiring sensitive data, which should be adequately protected from unauthorized access. Integrity will ensure that the information sent (made available) to, for example, citizens has not been fabricated. This will translate into maintaining an appropriate level of efficiency of the state's activities in cyberspace. Availability will guarantee the appropriate volume of data and information that is required for information systems and the state to function normally.

As can be seen, the state, when undertaking activities in cyberspace, acts multidimensionally. In addition to self-powering the information systems it uses, it also seeks to obtain information and data from citizens by enabling them to remotely use its resources, particularly those of IT. It also seeks to adequately secure all processes related to this sector of its activities by introducing appropriate organizational and technical solutions that determine the level of information security. By analyzing the above premises, it can be concluded that communication is an important factor linking the level of state security with activities in cyberspace. This is because the lack of adequately qualitative communication or its disruption can lead to misunderstandings that can result in vulnerabilities. Their occurrence will intensify the effects of potential threats.

## **CITIZENS VS CYBERSPACE**

In the era of ever advancing technical and technological development, single individuals (citizens) are generating ever-increasing volumes of data. This is related to the transfer of daily

---

<sup>16</sup> Ibidem, p. 17.

<sup>17</sup> Polski Komitet Normalizacyjny, *Polska Norma PN-EN ISO/IEC 27001*, Warszawa 2018, p. 4.

performed tasks such as, for example, placing an order in a store or preparing documents to digital reality. Currently, the following categories of activities undergoing digitization can be identified:

- Private,
- Official,
- Administrative.

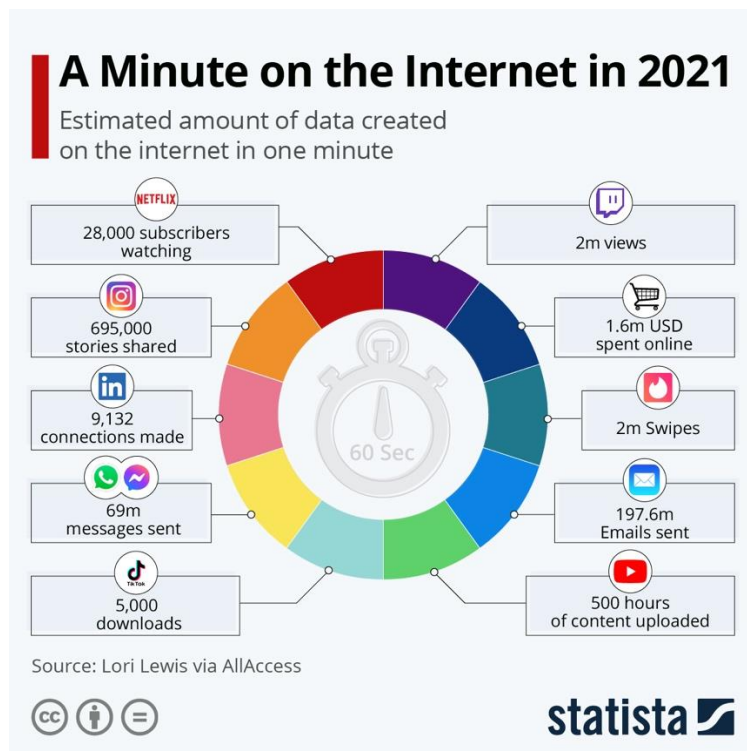
The first will include all activities undertaken to achieve personal goals. These will be, for example, shopping, reading the news or checking the weather. The second category will consist of activities whose implication is the due performance of business duties. This could be, for example, the preparation of project documentation or business meetings. The last group will be administrative activities, that is, all activities on the citizen-state line. In this category we can include such activities as paying taxes, filing administrative applications and statements, verifying social security. The above categories can function independently, however, more and more emphasis is being placed on their integration which allows building comprehensive digital services for citizens<sup>18</sup>.

Fig. 1.

Amount of data generated online per minute

---

<sup>18</sup> K. Lorenz, *Podpis zaufany w rozwoju e-administracji*, „Studia Informatica Pomerania” 2017, vol. 45, no. 3, p. 25-28. <https://doi.org/10.18276/si.2017.45-03>



Source: Statista, <https://www.statista.com/>, „A Minute on the Internet in 2021” (accessed: 21.07.2022).

The generation of large amounts of diverse data in a short period of time (Figure 1) by citizens will enable their algorithmization. This will be possible through the use of Big Data class systems that aggregate and analyze data in any form (structured data, images, texts, videos, etc.)<sup>19</sup>. They operate according to the principles of the four Vs (volume, velocity, variety, value). The volume, i.e. the amount of data produced, is practically doubling from year to year in the digital age. The velocity of their processing is limited by the technological solutions used and material resources (including financial). Variety the multitude of types of data carriers. Value, i.e. the quality of the data held that we intend to use to generate a given algorithm<sup>20</sup>. However, it should be noted that the automation of taking actions based on the inputs (data and information) received from the user may create a number of complications. The main risk associated with the aforementioned phenomenon will involve loss of control over one's data<sup>21</sup>. This can contribute to the theft of an individual's identity which will allow an adversary to gain access to services and data and information normally unavailable to them<sup>22</sup>. Reduced scoring

<sup>19</sup> J. Wieczorkowski, I. Chomiak-Orsa, I. Pawełoszek, *Big Data w marketingu — narzędzie doskonalenia relacji z klientami*, „Marketing i rynek” 2022, vol. 39, no. 1, p. 4-5. <https://doi.org/10.33226/1231-7853.2022.1.1>

<sup>20</sup> SAS, <https://www.sas.com/>, „Big Data. What it is and why it matters” (accessed: 21.07.2022).

<sup>21</sup> K. Szymielewicz, K. Iwańska, *Śledzenie i profilowanie w sieci*, Fundacja Panoptikon, Warszawa 2019, p. 4.

<sup>22</sup> Ibidem, p. 5.



will also be a risk resulting from the automation of data processing. An affected citizen may find it difficult to access basic services (financial, insurance or administrative), as he or she will be indicated by the algorithm as a suspicious person<sup>23</sup>. The build-up of these threats can lead to an individual's increasing vulnerability to disinformation activities. This will allow opponents to shape its future actions with, for example, fake information (so-called "fake news"), in order to achieve their stated goal<sup>24</sup>.

By analyzing the above rationale, it can be seen that, as in the case of an organization (state), the actions of citizens should be aimed at securing the data they share. Failure to implement appropriate safeguards will translate into the possibility of unauthorized use. This can even lead to a disruption of the level of security of the state through the unconscious use of citizens for military purposes<sup>25</sup>.

Actions taken by individuals in cyberspace, in addition to the subject dimension, can also be analyzed by the age of the system user. This is because different actions in cyberspace will be performed by a child or young person and by adults. Currently, we can distinguish three age categories of users of the digital environment:

- Children and adolescents,
- Adults,
- Seniors<sup>26</sup>.

The first group will focus its activities in cyberspace on obtaining materials related to entertainment in the broadest sense. These activities can be categorized as private. In this age group, special attention should be paid to the formation of an appropriate organizational and legal framework to protect children and adolescents from accessing inappropriate content<sup>27</sup>. The activities of adults in cyberspace will focus on the entire subject spectrum of digitized activities (private, official and administrative). This has to do with their entry into the working age, which obliges adults to start working and reporting to the state, e.g. by filing a PIT form (an element of citizen financial reporting). Seniors, on the other hand, will use cyberspace to

---

<sup>23</sup> Ibidem, p. 32.

<sup>24</sup> Ibidem, p. 33.

<sup>25</sup> M. Grzelak, K. Liedel, *Bezpieczeństwo w cyberprzestrzeni. Zagrożenia i wyzwania dla Polski – zarys problemu*, „Bezpieczeństwo Narodowe” 2012, vol. 2, no. 22, p. 128.

<sup>26</sup> Centrum Badania Opinii Społecznej, <https://www.cbos.pl/>, „Korzystanie z Internetu” (accessed: 21.07.2022).

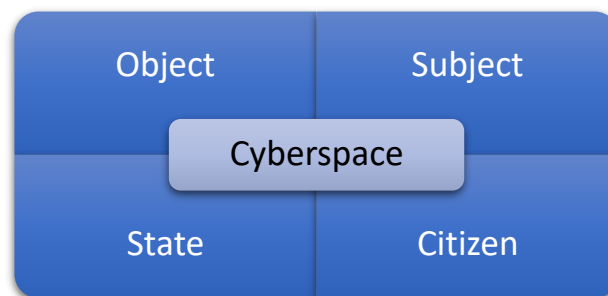
<sup>27</sup> M. Olchanowski, *Bezpieczeństwo dzieci i młodzieży w cyberprzestrzeni na podstawie Krajowych Ram Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022*, „Zeszyty Naukowe Zbliżenia Cywilizacyjne” 2017, vol. 13, no. 3, p. 59-62.

carry out private-administrative matters related not only to reporting to the state, but also to maintaining their quality of life (e.g., making medical appointments, registering for cultural events)<sup>28</sup>.

Analyzing the above factors, it can be seen that the subject and entity activities in cyberspace by the state and citizens intermingle. This phenomenon is illustrated in Figure 2.

Fig. 2.

Intersection of actions taken in cyberspace



Source: Own study.

The combination of the aforementioned elements will allow the complementary conduct of activities aimed at mitigating the level of risk of cyber threats that could affect not only citizens, but also the state itself. It should, however, be borne in mind to adapt the regulations being prepared to the appropriate typology of activities undertaken in cyberspace. Excessive generalization of the designed solutions may lead to information noise associated, for example, with decision-making paralysis, which will amplify the possibility of using vulnerabilities to exploit an individual, entity or system (network).

### **THE IMPACT OF CITIZENS' CYBER SECURITY ON STATE SECURITY**

State security can be defined in two ways. As a certain stable condition in which the sovereignty of the state is not threatened and society can develop without any disturbances (threats). We can also express state security by the ratio of defense potential to the scale of threats, i.e. organized defense against possible threats<sup>29</sup>. Analyzing the definitions of national

---

<sup>28</sup> K. M. Błęszyńska, M. Orłowska, *Seniorzy w cyberprzestrzeni. Między stereotypem a rzeczywistością*, „Studia edukacyjne” 2020, no. 56, p. 155-160. <https://doi.org/10.14746/se.2020.56.8>

<sup>29</sup> W. Łępkowski (redakcja naukowa), *Słownik terminów z zakresu bezpieczeństwa narodowego*, Warszawa 2010, p. 16.

security, it can be concluded that they are the same as the definition of state security<sup>30</sup>. Cyber security, on the other hand, is a set of all techniques, processes, and measures (information resources) whose use is aimed at preventing the occurrence of breaches of computer systems in the broad sense, electronic communications, as well as the data and information processed in them<sup>31</sup>. Analyzing the definitions presented above, it can be seen that cyber security will be one of the subject criteria of national (state) security. Thus, the holistic model of national security proposed by Professor Waldemar Kitler, which illustrates the relationship between different types of security in terms of subject matter, will change. This change is illustrated in Figure 3.

Fig. 3.

Holistic model of national security with the inclusion of cyber security



Source: own study based on W. Kitler, *Zakres bezpieczeństwa państwa (narodowego)*, [in:] *Identyfikacja, klasyfikacja, podział i uzasadnienie pojęcia, istoty, składników i zakresu bezpieczeństwa państwa (narodowego)*, (eds.) J. Gryz, W. Kitler, Wydawnictwo Akademii Obrony Narodowej, Warszawa 2014, p. 27 (Scope of state (national) security, ... Identification, classification, division and justification of the concept, essence, components and scope of state (national) security)

<sup>30</sup> Vide, D. Saukens, *Zależności między pojęciami bezpieczeństwo państwa a bezpieczeństwo narodowe*, [in:] *Humanistyka i nauki społeczne. Doświadczenia. Konteksty. Wyzwania.*, (ed.) K. Pujer, Wydawnictwo Naukowe Exante, Wrocław 2020.

<sup>31</sup> „Słownik kluczowych pojęć z zakresu cyberbezpieczeństwa”, Portal Gov.pl, <https://www.gov.pl/>, (accessed: 21.07.2022).

The intersection of the national security environment and cyber security will lead to a direct link between the two. Thus, it can be concluded that the level of cyber security will play an important role in shaping national security. However, it should be noted that the sustainability of the above link depends on the specific actions taken by users and their impact on the security of processed data and information. After all, it is they (in the person of citizens) who will constitute the first line and at the same time the last line of defense of the system in use.

Currently, users of information systems (citizens) may be exposed to two types of threats coming from cyberspace (Table 3). These are technical threats and social threats. Social threats will directly affect the person who is affected. The actions taken by the adversary will focus on using the technical elements of the information system to launch an attack. In turn, they will not themselves be its target. The opposite situation can be observed in the case of technical threats, where the adversary, using IT tools, tries to damage the information system under attack, or take over the data and information processed in it.

Table 3  
Types of cyber threats

Non-technical (social) risks	Technical risks
Cyberstalking, Trolling, Flaming, Cyberprostitution, Sexting, Grooming	Viruses, Worms, DoS, Spyware, Malware, Trojan Horses, etc.

Source: Portal Gov.pl, <https://www.gov.pl/>, „Dla każdego – cyberhigiena” (accessed: 21.07.2022).

These two categories of cyber threats can be combined with each other to get the best result of the attack<sup>32</sup>. The threat typology in Table 3 can be supplemented by cyber threats, which are a combination of technical and social threats. These can include, for example, phishing or ransomware. After all, in order to carry out these attacks, the adversary must use not only IT tools, but also elements of social engineering, i.e. directly affect the selected victim (person).

Analyzing the above conditions, it can be seen that the threats coming from cyberspace will affect not only the users themselves, but also information systems. This two-faceted approach will directly translate into a reduction in the effectiveness of actions taken by citizens

---

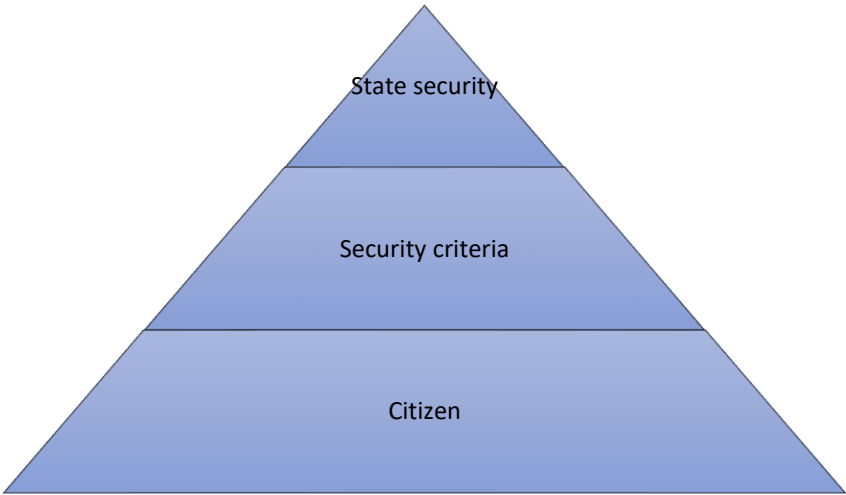
<sup>32</sup> An attack should be understood as a set of all activities that lead to unauthorized access to an IT system or obtaining data and information.

in cyberspace regardless of their subject or entity location. It will also result in a reduction in the level of their cyber security.

The use by citizens to carry out activities in cyberspace of information systems provided by the state, if they are the target of an attack, may affect the level of state security. This is because an attacker can, by taking advantage of a user's lack of attention, gain access to sensitive data or a system, which will provide a foothold for reconnaissance of the IT infrastructure and further propagation of the attack using a different vector (method of attack). The release to the public, for example, of unauthorized data obtained in an unauthorized manner can even lead to a disruption of the continuity of state operations through the creation of new vulnerabilities.

As can be seen from the above, the level of cyber security of citizens will correlate directly proportionally with the level of state security. This has to do with the ever-increasing computerization and related digitalization. The progressive networking not only of social relations, but also of administrative ties on the citizen-state line will also contribute to this. However, it should be pointed out that a person (citizen) will always be the foundation for all activities related to ensuring cyber security or national security. This is illustrated in Figure 4.

Fig. 4.  
Citizen in the system of ensuring state security



Source: Own study.

This is because at present it is the only creative force capable of creating new, original solutions (tools, systems, etc.). Without man (citizen, user, operator) it would be impossible for all systems to function, including the state.

## **CONCLUSION**

Due to the rapidly advancing technological and technical progress, more and more threats affecting countries as well as their citizens will come from cyberspace. They will affect the operation not only of the individuals or entities directly involved, but also of other components of selected systems. It therefore becomes necessary to examine how these threats will impact the security of citizens or the state.

Analyzing the assumptions made in the article, it can be concluded that the actions taken by citizens in cyberspace will affect the formation of the level of state security. However, it is not possible to state unequivocally which actions are most important for ensuring national security. However, it should be noted that the level of cyber security of citizens will directly influence the level of state security. This impact is possible due to the synergy of private and public information systems, which will be affected (to varying degrees) by the same cyber threats.

Due to the universality of threats from cyberspace, it becomes an important factor to control the level of cyber security of citizens, who are the first line of defense against the escalation of attacks. To this end, it is necessary to implement appropriate organizational and legal regulations that will determine the possibility of using IT tools to counter cyber threats. This will make it possible to level the information noise that could occur, should there be decision paralysis. The prepared guidelines will also provide assistance to policymakers when making decisions in connection with the materialization of threats emanating from cyberspace.

## **REFERENCE LIST**

### **LITERATURE**

- Błęszyńska K. M., Orłowska M., *Seniorzy w cyberprzestrzeni. Między stereotypem a rzeczywistością*, „Studia edukacyjne” 2020, no 56. <https://doi.org/10.14746/se.2020.56.8>
- Dudek D., Husak Z., Kowalski G., Lis W., *Konstytucyjny system organów państwa*, Wydawnictwo C.H. Beck, Warszawa 2012.

- Grzelak M., Liedel K., *Bezpieczeństwo w cyberprzestrzeni. Zagrożenia i wyzwania dla Polski – zarys problemu*, „Bezpieczeństwo Narodowe” 2012, vol. 2, no 22.
- Iwasiński Ł., *Społeczne zagrożenia danetyzacji rzeczywistości*, [in:] *Nauka o informacji w okresie zmian. Informatologia i humanistyka cyfrowa*, (ed.) B. Sosińska-Kalata, Wydawnictwo Naukowe i Edukacyjne SBP, Warszawa 2016.
- Kitler W., *Zakres bezpieczeństwa państwa (narodowego)*, [in:] *Identyfikacja, klasyfikacja, podział i uzasadnienie pojęcia, istoty, składników i zakresu bezpieczeństwa państwa (narodowego)*, (eds.) J. Gryz, W. Kitler, Wydawnictwo Akademii Obrony Narodowej, Warszawa 2014.
- Krukowski J., *Wstęp do nauki o państwie i prawie*, Wydawnictwo Towarzystwa Naukowego Katolickiego Uniwersytetu Lubelskiego Jana Pawła II, Lublin 2004.
- Liderman K., *Bezpieczeństwo informacyjne. Nowe wyzwania*, Wydawnictwo Naukowe PWN, Warszawa 2017.
- Lorenz K., *Podpis zaufany w rozwoju e-administracji*, „Studia Informatica Pomerania” 2017, vol. 45, no 3. <https://doi.org/10.18276/si.2017.45-03>
- Łepkowski W. (redakcja naukowa), *Słownik terminów z zakresu bezpieczeństwa narodowego*, Akademia Obrony Narodowej, Warszawa 2010.
- Marczyk M., *Cyberprzestrzeń jako nowy wymiar aktywności człowieka – analiza pojęciowa obszaru*, „Przegląd teleinformatyczny” 2012, vol. 6, no 1-2.
- Mindur M., *Wpływ postępu technicznego i technologicznego oraz wydarzeń politycznych na rozwój gospodarki globalnej*, „Logistyka” 2012, vol. 3.
- Olchanowski M., *Bezpieczeństwo dzieci i młodzieży w cyberprzestrzeni na podstawie Krajowych Ram Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022*, „Zeszyty Naukowe Zbliżenia Cywilizacyjne” 2017, vol. 13, no 3.
- Rostek K., Gołuch-Trojanek K., *Standaryzacja procesów i jej rola w procesie wdrażania zintegrowanych systemów informatycznych w instytucjach publicznych: (na przykładzie uczelni publicznej)*, „Autobusy: technika, eksploatacja, systemy transportowe” 2017, vol. 18, no 9.
- Saukens D., *Zależności między pojęciami bezpieczeństwo państwa a bezpieczeństwo narodowe*, [in:] *Humanistyka i nauki społeczne. Doświadczenia. Konteksty. Wyzwania.*, (ed.) K. Pujer, Wydawnictwo Naukowe Exante, Wrocław 2020.
- Szymielewicz K., Iwańska K., *Śledzenie i profilowanie w sieci*, Fundacja Panoptykon, Warszawa 2019.
- Wieczorkowski J., Chomiak-Orsa I., Pawełoszek I., *Big Data w marketingu – narzędzie doskonalenia relacji z klientami*, „Marketing i rynek” 2022, vol. 39, no 1. <https://doi.org/10.33226/1231-7853.2022.1.1>

## SOURCES

- Centrum Badania Opinii Społecznej, <https://www.cbos.pl/>, „Korzystanie z Internetu”.
- Główny Urząd Statystyczny, <https://stat.gov.pl/> „Społeczeństwo informacyjne w Polsce w 2021 r.”.
- Polski Komitet Normalizacyjny, *Polska Norma PN-EN ISO/IEC 27001*, Warszawa 2018.
- Portal Gov.pl, <https://www.gov.pl/>, „Dla każdego – cyberhigiena”.
- Portal Gov.pl, <https://www.gov.pl/>, „Słownik kluczowych pojęć z zakresu cyberbezpieczeństwa”.

SAS, <https://www.sas.com/>, „Big Data. What it is and why it matters”.

Statista, <https://www.statista.com/>, „A Minute on the Internet in 2021”.

Strona internetowa NIK, <https://www.nik.gov.pl/>, „Standardy Kontroli NIK”.

---



Copyright (c) 2022 Michał JUREK



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