GIS Odyssey Journal

2021 • Volume 1 • Number 1

https://doi.org/10.57599/gisoj.2021.1.1.91

Jerzy Stanik[1], Maciej Kiedrowicz[2]

ORGANIZATIONAL SECURITY SYSTEM AS A DETERMINANT OF ENHANCING SECURITY CULTURE OF GIS

Abstract: The purpose of this paper is to propose a way to measure security culture as a determinant of organizational safeguards for sensitive resources in GIS-class systems. Based on a critical analysis of the results of the risk estimation of sensitive resources in GIS, a variant of the model and then the methodology for measuring security culture was proposed, its basic elements were described, and then the criteria that should be met by each organizational safeguard, considered in the measurement of security culture, were identified and established. Based on the developed model of security culture measurement, methods for measuring this phenomenon in GIS from the perspective of the organizational safeguard system are indicated. Attention was focused on theoretical aspects and elements of best practice that indicate the feasibility of developing and applying a security culture model to measure security performance of GIS.

Keywords: safeguard system, risk, security culture model, roles and responsibilities in developing a security culture

Received: 8 July 2021; accepted: 3 August 2021

[1] Military University of Technology, Faculty of Cybernetics, Institute of Computer and Information Systems, Warsaw, Poland, ORCID ID: 0000-0002-0162-2579, email: jerzy.stanik@wat.edu.pl
[2] Military University of Technology, Faculty of Cybernetics, Institute of Computer and Information Systems, Warsaw, Poland, ORCID ID: 0000-0002-4389-0774, email: maciej.kiedrowicz@wat.edu.pl

Introduction

The issues of security culture and cyber security are not among the most important research areas related to GIS-class systems. Merely a few percent of the research carried out is related to this topic (see: The report on the implementation of the Task 1.5. as part of the project: the National Security System of the Republic of Poland, Warsaw-Siedlce, 2013). The statistics are very unfavourable, especially in terms of high social and financial costs associated with safeguarding spatial data processed in GIS-class computer systems. A security system of a ICT network of GIS must be strong enough to deal with 95% of basic cyber threats. Identifying and reacting quickly to the remaining 5% of cyber threats consumes half of the budgets for technical and organizational safeguards. No wonder that budgets for the security of GIS spatial information are growing. Today, strategies in GIS systems are much more closely related to information security than ever before. Fortunately, management boards of companies offering GIS-class solutions understand the need to invest in security more and more. Security issues are constantly moving forward, evolving, changing. This area is certainly different than even a few years ago. All because the landscape of potential or real threats becomes somewhat simplified, and malware is becoming more and more effective in its basic principle of operation – the code simply has to get inside the network, take control of the device and do what it was created for. At the same time, the security of the ICT network of GIS has to be more and more sophisticated – you need to understand which systems talk to each other and what it means.

The research priorities in the field of GIS security in the European Union include research on shaping a security culture by introducing appropriate functions of security culture, which such functions strengthen the role, of an organizational nature, of the security system, and by disseminating scientific discoveries and examples of good practice in this field (Cieślarczyk, 2010, 2012). The basic pillar of the global strategy in the field of the GIS security is building and maintaining a security culture and safeguarding systems at a high level of quality and effectiveness, and applying a system approach to the issues of security culture at the organizational level.

The purpose of this paper is to propose a way to measure security culture as a determinant of organizational safeguards for sensitive resources in GIS-class systems. Based on a critical analysis of the results of risk assessment of sensitive resources in GIS, a variant of the security culture measurement model was proposed, its basic elements were described, and then the criteria that should be met by each organizational safeguard, taken into account in the measurement of security culture, were identified and established. Based on the developed model of security culture measurement, a method for measuring this phenomenon in GIS from the perspective of the organizational safeguard system was indicated.

Model of GIS system for measuring the security culture

The most general definition of GIS is an organized set of computer hardware, software, spatially referenced data and people (contractors and users) created to

effectively collect, store, share, process, analyze, visualize all geographic data. The graphic illustration of the GIS system for measuring the security culture is shown in Figure 1.

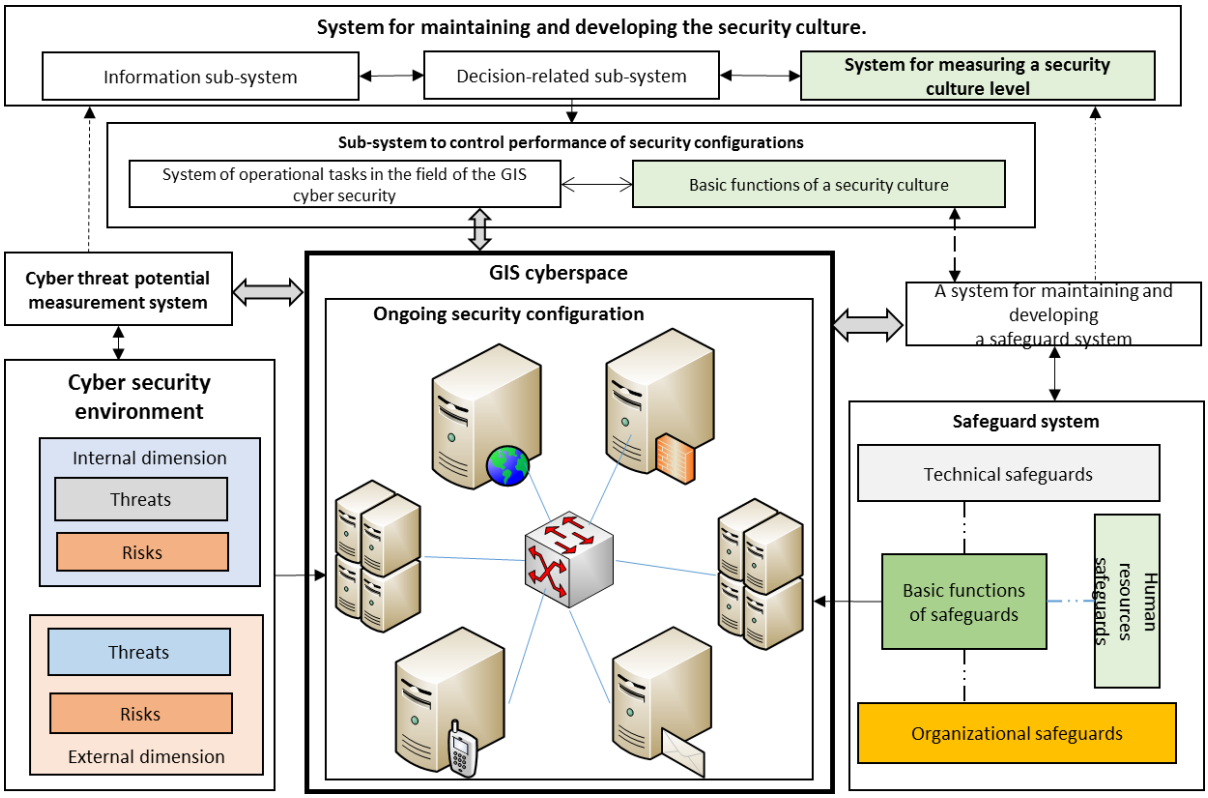

Fig.1. The graphic illustration of the GIS system for cyber security
Source: the in-house elaboration

This figure emphasizes the four important elements:

1. The GIS cyber space and its current security configuration.
2. A real cyber security environment in the external and internal dimensions.
3. The safeguard system.
4. A system for maintaining and developing the security culture.

In the systems approach, the GIS cyber space is considered to be an open system. The openness of the system is that it exchanges information with the environment – the cyber security environment (Sienkiewicz, 2015). The systemic approach to the analysis of GIS cyber space forces to treat it as a compact structure with various inputs and outputs. Inside this structure are smaller elements, treated as systems or subsystems that enable the processing of inputs into outputs in accordance with the objectives of the security culture within a GIS cyber space.

According to Gaździcki (2010), Spatial Data will be referred to as data describing spatial objects, including phenomena and processes present or occurring in an assumed spatial data system. The spatial data apply to:

- geometric properties of the spatial object, especially its location relative to the adopted two-dimensional or three-dimensional coordinate system,

- object characteristics in relation to time, e.g. its creation date,
- spatial (topological) relationships of the object with other spatial objects,
- highlighted descriptive attributes of the spatial object, used for its identification and defining its basic properties.

The real GIS cyber security environment in the external and internal dimensions is created by cyber threats and risk factors in the area of GIS cyber security. Among the cyber threats, particularly important are those concerning the critical infrastructure of GIS spatial data and its essential subsystems, controlled by systems for operating tasks. Operational tasks aimed at achieving the strategic goal of ensuring the required level of security culture and ensuring an acceptable level of GIS security in cyber space. The main operational tasks include (Gwoździewicz & Tomaszycki, 2017):

- identifying real and potential sources of cyber threats, including through international information exchange,
- continuous risk analysis in relation to important objects of GIS critical infrastructure,
- activities in the field of cryptography and cryptanalysis to secure sensitive information resources and identify potential threats from hostile actors,
- ongoing monitoring of critical points of the safeguard system, particularly vulnerable to cyber attacks, especially through the use of task force teams for IT security incident responses,
- audit of cyber security measures and mechanisms, taking into account the adopted standards,
- preparation and implementation of scenarios of conduct in the event of cyber attacks against digitized data and GIS tasks;
- developing and updating – from the point of view of cyber security – crisis response plans and operational plans for functioning during a cyber threat or cyber attack,
- conducting active cyber defense – and, as part of the cyber defense, offensive activities in cyber space – and maintaining cyber war readiness,
- protection and defense of internal ICT systems and resources stored within these systems,
- supporting other key actors of GIS activities in the field of their cyber security,
- counteracting and combating cyber crime,
- ongoing information and education activities addressed to the public in the field of a secure use of cyber space and information about identified threats.

In this respect, intentional attacks on communication (telecommunication) systems ensuring the efficient functioning of the information security control sub-system, the defense sub-system – the security system, and support sub-systems, may be extremely dangerous for the GIS cyber space.

A GIS security system is defined as a set of security features and a set of relationships between them that ensure a specific performance of the security system. The scope and purpose of the security system is specified in a set of basic security functions. In the simplest terms, security measures are all kinds of practices, procedures, and mechanisms that reduce the risks associated with unauthorized access

to, modification of, destruction of, or total loss of GIS spatial information. Effective protection usually requires the implementation of technical, organizational or personnel security measures in combination with security procedures defining the basic rules of behavior and conduct in relation to GIS entities. Basic functions of safeguards include (Krupa et al., 2018; Prauzner, 2012):

- protection against cyber threats,
- deterring intruders,
- reduction of the impact of vulnerabilities,
- limiting the aftermath,
- detection of security incidents and their prevention,
- facilitating the recovery of violated resources,
- awareness-raising,
- training,
- monitoring,
- remedial and corrective actions.

The system of maintaining and developing a security culture is defined as a set of tasks and connections between them, the performance of which enables the defense and protection of ICT systems in cyber space of GIS while maintaining the efficiency and flexibility of the implementation of processes and tasks performed with the use of these systems. The most important preparation (preparatory) tasks in the area of cyber security of GIS include the implementation and development of a systemic approach to cyber security in the legal, organizational, technical dimensions and the phenomenon of security culture (Kowal et al., 2015). As part of maintaining and developing a cyber security culture of GIS, it is particularly important to:

- development and implementation of rules and procedures (also the so-called good practices) for managing the cyber security culture,
- continuous modernization of the elements of the management sub-system, including the implementation of safe means of management,
- building an independent communication network for security management of GIS and ensuring effective control of ICT systems of GIS,
- developing minimum cyber security standards for critical infrastructure of GIS,
- developing plans for exercises and training for cyber security of GIS,
- identifying requirements and goals for education, information, and research programs.

The preparation (maintenance and development) of the operational cells of the cyber security system of GIS should be aimed at ensuring resources and competences appropriate to the dynamically changing operational needs in the cyber security environment. It is therefore important:

- to create protective and defensive mechanisms to adapt quickly to changes in the cyber security environment, to be able to respond to unforeseen situations, such as Cyber attacks,
- to obtain the capacity to efficiently manage the resources of the security system of GIS,

- to ensure the secure flow of information between links of cyber space of GIS,
- to build the capacity to conduct proactive activities in the cyber space of GIS,
- to maintain the basic functions of security culture of GIS,
- to acquire data to measure security culture of GIS.

Security culture of GIS

It is possible to think about security culture of GIS in a simplistic way, or to try to understand the essence of the phenomenon in more detail. Let us start with the simplest way of understanding this concept. The studies conducted so far show (Shaw & Blewitt, 1996) that the security culture of GIS is – generally speaking – its knowledge base and ways of thinking about its security, characteristic of a given subject of activity, e.g. an organization. An extensive definition of security culture: "a pattern of basic assumptions, values, norms, rules, symbols and beliefs, influencing the way challenges, opportunities and (or) threats are perceived, as well as the way security is felt and thought about, and the related way subjects behave and act (interact), variously 'learned' by these subjects and articulated in the processes of broadly understood education, including also in the natural processes of internal integration and external adaptation, as well as in other organizational processes, and also in the process of strengthening of defence in the broad (not only military) sense, serving the harmonious development of these entities and achieving by them the broadest sense of security, to the benefit of themselves, but also the environment" can be found in Cieślarczyk (2010). For the purposes of this paper, we will adopt the following definition: "Security culture of GIS is the totality of the material and non-material output of a specific GIS actor, e.g. a human being, which serves its broadly defined defense. It is used *de facto* to maintain (cultivate), recover (when lost) and enhance the security level of critical infrastructure systems of GIS". It consists of the following three dimensions – the first: mental-spiritual, the second: organizational-legal and the third dimension: material (Fig. 2).

The equivalent of security culture are three pillars (mental, organizational and material) of the broadly understood defense of a given actor. Identifying the concept of security with the potential of defense – a response system or security system – is close to one of the definitions of security formulated by the securitologist – Korzeniowski (2000): "Security is the subject's ability to be creative and denotes the objective state consisting in the absence [or neutralization] of the threat". Secondly, we can treat security not only as a specific state of affairs, but also as a value (Piwowarski, 2010), as well as – in the third variant: a function or process of (not endangered) development. The second and third way of understanding the concept of security (value, development process) allows to compare them with the phenomenon of security and defense culture, and even assume that they are identical.

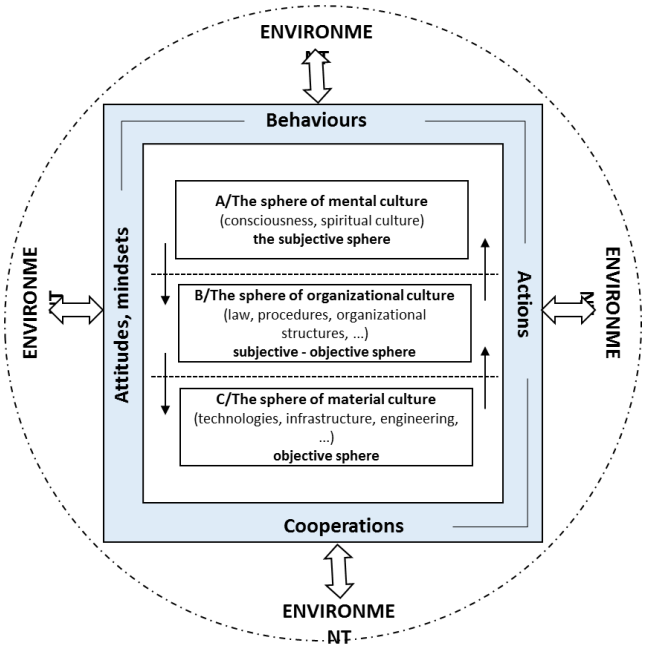

Fig. 2. Pillars of security culture
Source: the in-house elaboration

In view of the aforementioned, we can assume that the Security Culture of GIS is based on the established values and development processes reflected in its three pillars, in the individual and collective dimensions, and the external and internal dimensions in relation to its two basic sub-systems: threats and defense – the Security System of GIS. The phenomenon of security culture can be looked at from yet another perspective, as Figure 3 tries to show.

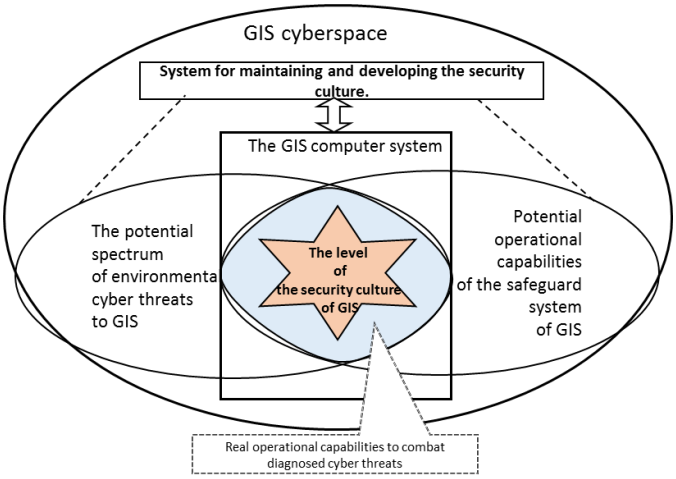

Fig. 3. Basic elements of the security culture model of GIS
Source: the in-house elaboration

In order to understand the structure of the security culture phenomenon of GIS, it is necessary to "look" inside its response/security system of GIS and to identify the potential or real capabilities of the cyber threat system. The potential operational capabilities of a security system of GIS and the potential spectrum of environmental cyber threats determine the individual elements of a security culture of GIS. A specific

core of the security culture of GIS is a system of values – real operational capabilities to combat diagnosed cyber threats of a given cyber security environment of GIS, the security culture of which we analyze. Another element of the safety culture are the standards that an entity follows to ensure its security in its various subject areas. Values and norms, together with the knowledge and way of thinking about security as well as emotional "qualifications" possessed by the subject of GIS, exert a great influence on the relations of the computer system of GIS with the environment, on its behavior, actions and interactions. This is especially important in difficult, crisis or cyber attack situations. This is where the security culture of GIS becomes apparent. A graphic presentation of this issue is the pyramid of security culture, which consists of the following elements: assumptions, norms and values, and artifacts (Fig. 4).

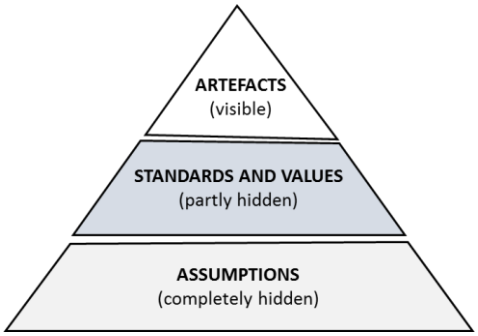

Fig. 4. Security culture pyramid
Source: the in-house elaboration

The visible manifestation of the GIS security culture are artifacts, among which the following can be distinguished:

- process and information artifacts (basic assets of GIS cyber space, in particular security system protection processes and security configurations of the computer system of GIS),
- behavioral artifacts (cyber threats, behaviors, habits),
- physical and organization artifacts (technical safeguards, organizational safeguards, human resources safeguards) (Stanik & Kiedrowicz, 2021; Stanik & Protasowicki, 2020).

A slightly deeper and, at the same time, less visible level of security culture of GIS are the norms and values in force in GIS cyber space. Their distinguishing feature is that they are more difficult to observe. Two categories can be distinguished among them: declared and followed. The declared categories are much easier to notice for others. Actors of GIS openly talk about what is important to them, what actions are worth following, and what requires criticism. On the other hand, the norms and values observed are more difficult to articulate. Very often there are situations where declarations made, for example regarding certain ways of proceeding, are not reflected in the actual manner of proceeding. The deepest level, and at the same time completely hidden, are assumptions. The assumptions are, in a way, the foundation of a security culture. Depending on what they refer to, they are divided into:

- assumptions about the nature of reality and truth – making it necessary to think about what constitutes the basis for the functioning of GIS,
- assumptions about the nature of time – indicating the time horizon (past, present, future) and the way, in which time is used, in cyber space of GIS,
- assumptions about human nature – general features of human character,
- assumptions about the nature of interpersonal relations – ideas about the correct ordering of formal and informal social relations,
- assumptions about the nature of the environment – the perception of the environment by the subject of operation of GIS, indicating the relationship between the GIS computer system and the environment (Stanik & Kiedrowicz, 2021; Stanik & Protasowicki, 2020).

Research methodology

The research presented in this paper is conceptual. This determines the lack of a research hypothesis. Nevertheless, this document assumes that the process of measuring the level of security culture of GIS will be successful (accurate) provided that the cyber space of GIS is divided into specific analytical dimensions. The basic research process led to the construction of a methodology for measuring the level of security culture and consists of three major stages. In the first stage, cyber security of GIS is broken down into diagnosis dimensions through a literature review in the areas of cyber space, cyber security and management. At this stage, the deductive approach dominates. In the next step, the authors define the cyber security environment – cyber threats and risk sources. Furthermore, at this stage, based on an extensive literature review (in the fields of IT, telecommunications, information security and cyber security, among others), only those elements that can be considered as a source of risk and those elements that make up the system for responding to cyber threats and cyber attacks – the security system of GIS – have been identified. Finally, a coherent model of security culture of GIS constructed by synthesizing isolated dimensions. In this context, cyber security of GIS can be divided into: the time-based dimension, the dimension of threatened resources, the dimension of threatened actors, the dimension of threatened assets of critical infrastructure of GIS, of the nature of information processes and resources, the dimension of the legal form of cyber security.

Methodology for studying the level of security culture

Figure 5 shows the methodology for testing the level of security culture of GIS. This methodology enables the security culture of GIS to be assessed at three levels of detail:

- Level I enables the analysis of the level of security culture in three layers: cyber security environment, GIS computer system, crisis response system, also known as the security system of GIS.
- Level II contains information on the level of security culture in terms of indicators in three areas: knowledge, skills and action.

- Level III is the most detailed and allows you to analyze the level of security culture in relation to individual cyber space assets of GIS.

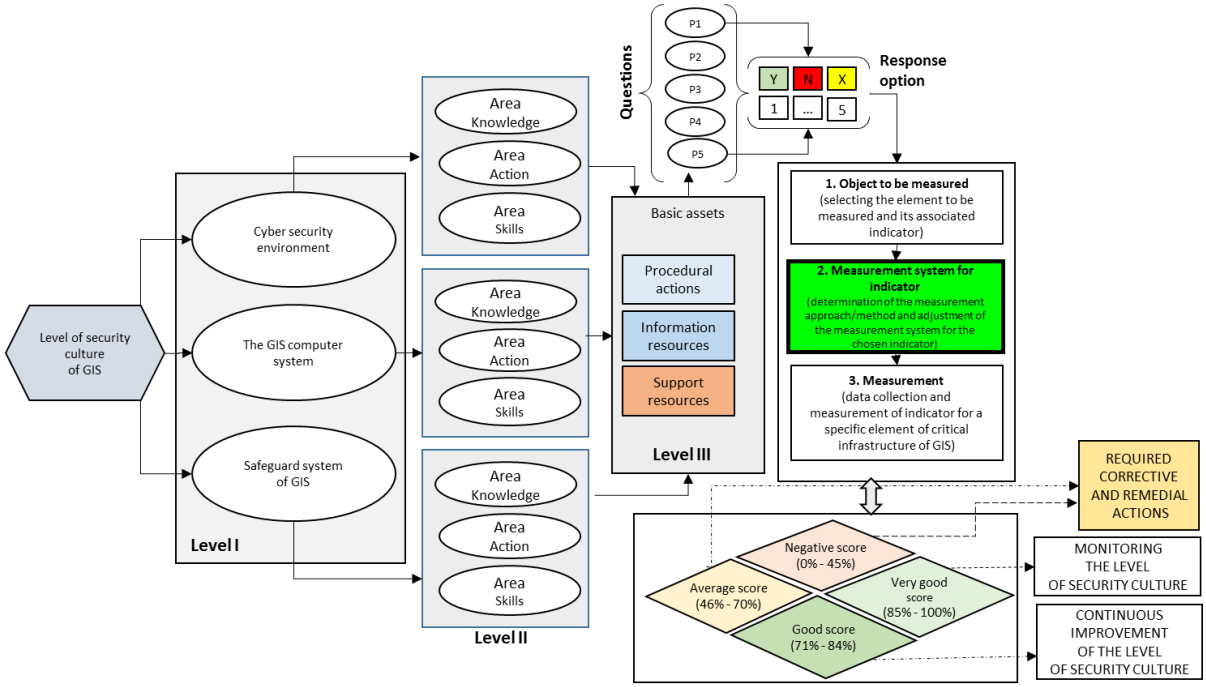

Fig. 5. Methodology for studying the level of security culture at work
Source: the in-house elaboration

Tools and methods for studying the level of security culture of GIS

When attempting to identify methods for assessing the level of GIS security culture, it is worth paying attention to the fact that mainly we are dealing with the measurement of qualitative features – therefore, difficult to estimate and evaluate (AbuShawar & Atwell, 2007; Gabryelewicz, 2017). The most questionable thing is to choose the right assets of GIS and assign them specific features and indicators/measures, and assign them appropriate weights and points. It depends on the perception of the actors of GIS or its subsystems/objects under study. Therefore, the methods presented are not completely perfect. The most common measurement problems are formulated with using the following questions:

- what are the key features of a security culture of GIS that can be measured?
- are the indicators for measurement of security culture of GIS the same for other entities of activity or should different evaluation criteria be used, taking into account the type or class of GIS, the current state of security culture?
- is there a direct relationship between the features of a security culture of GIS and the state of its security system, do they affect, for example, the risk level indicator?

In the view of the above questions, there is an interest in measuring the security culture and disseminating assessment tools in the form of questionnaires developed for the internal needs of GIS systems. The analysis of the professional literature and the review

of the tools used to measure the security culture of GIS shows that the main subjects of interest are:

- assessment of the perception of the current state of selected aspects of GIS functioning (elements of critical infrastructure, management system, security system, secure operation procedures, competence of personnel or users of GIS),
- individual feelings of employees or GIS users – optimism, pessimism),
- individual types of behavior in the cyber security environment (taking risk, violating applicable rules, reporting security breaches).

Security culture assessment is the assessment of “invisible” norms and assumptions with using “visible” indicators. The most frequently used indicators used to assess the organization's security culture are: management commitment, security training, motivation, security rules, accident records, effectiveness of the control and communication system, well-designed technical equipment. Based on the proposed methodology, two methods were developed to assess the level of security culture in GIS: indicator method, grid method.

Indicator-based method

The example method for assessing the level of cyber security culture of GIS refers to the safeguard system of GIS and considers two types of security status indicators: "outcome indicators" and "activities indicators". The term "security performance indicators" is used to mean observable measurements which provide an insight into the security status of a security system that is difficult to measure directly. The performance of the safeguard system in a GIS should be measured so that the assessment is objective. The security of the safeguard system of GIS cannot be measured directly, so measures (security performance indicators) are necessary. Two types of security performance indicators will be presented in this paper: "outcome indicators" and "activities indicators".

Outcome indicators are intended to help in assessing whether the activities related to the security of the security system (policies, procedures and practices, security measures, safeguards, etc.) lead to the achievement of the intended results, and whether such measures in fact lead to a lower probability of occurrence. incident or cyber attack. They are reaction-based, aim to measure the impact of actions taken to manage cyber security, and are similar to what other documents refer to as "lagging indicators". Outcome indicators often measure a change in security over time or a poor state of security. Thus, the outcome indicators tell you whether the expected results were achieved (or whether the expected security-related result was not achieved). However, unlike activity indicators, they do not show why the result was achieved or not.

The activities indicator are intended to help determine whether administrators of GIS information system and cyber space services are taking actions that are deemed necessary to reduce the risk of losing essential elements of the critical infrastructure of GIS. Activities indicators provide guidance for actions and are similar to what other documents refer to as "leading indicators". Activities indicators often measure security

performance according to a tolerance level that shows deviations from the expected security status at a particular point in time. The activities indicators used this way emphasize the need for activities to increase the effectiveness of critical security measures (effectiveness of technical and organizational safeguards) when the tolerance level is exceeded. Thus, activities indicators provide companies with a means of regularly and systematically checking that they are implementing priority actions on a regular basis. Activities indicators can help explain why the outcome (e.g. as measured by an outcome indicator) was or was not achieved. An example of assigning outcome and activities indicators to selected utility attributes in relation to the set of elements of the security system of GIS, including policies, personnel and general risk management, is illustrated in Tables 1 and 2.

Table 1. Examples of activities indicators

	Security	Y/N I do not know	Quality	Y/N I do not know
Policies	Is the Security Policy reviewed and updated in accordance with established procedures?	Y	Is the distribution of roles and responsibilities between all directors and security-related employees clear and adequate?	Y
Practices	Is the Security Policy reviewed and updated in accordance with established procedures?	N	Is the distribution of roles and responsibilities between all directors and security-related employees clear and adequate?	Y
Leadership	Is the Security Policy reviewed and updated in accordance with established procedures?	I do not know – X	Is the distribution of roles and responsibilities between all directors and security-related employees clear and adequate?	N
Personnel	Is the distribution of roles and responsibilities among employees in security-related positions clear and adequate?	Y	Is the overall level of employee competency appropriate?	I do not know – X
Review and evaluation	Is the distribution of roles and responsibilities between all directors and security-related employees clear and adequate?	N	Is the overall level of employee competency appropriate?	Y

Source: the in-house elaboration

Table 2. Examples of outcome indicators

	Security	Continuity of operations	Quality	Scale [0 - 5]
Policies	The extent to which employees act in accordance with the Security Policy		The extent to which management takes the Quality Policy into account	3
Objectives	The extent to which security-related objectives are appropriate in relation to the current risks	The extent to which objectives related to continuity of operations are reviewed and updated in relation to established procedures	The extent to which quality objectives have been achieved	2
Leadership	The extent to which employees consider management to be a trusted source of information on risk and security	The extent to which employees consider management to be a trusted source of information on risk and security	The extent to which management supports the Quality Policy	4
Personnel	The extent to which employees have been trained in accordance with the planned training programme	The extent to which employees have been trained in accordance with the planned training programme	The extent to which employees are satisfied with the quality status of the company	1
Review and evaluation	The extent to which audits and technical controls are carried out in relation to the number of planned ones.	The extent to which continuity-of-operations status indicators are measured in a timely manner.	The extent to which audits and technical controls are carried out in relation to the number of planned ones.	2

Source: the in-house elaboration

There are several ways to assess the level of security culture of a GIS system. The simplest is to answer each question with “YES”/”NO” and calculate the percentage of “NO” answers in the whole list – a higher percentage indicates a lower level of security culture. A more reliable assessment is obtained by grading the answers and assigning appropriate values to them, e.g: Yes – 1, Rather yes – 2, To some extent – 3, Rather not – 4, No – 5. A higher aggregate value indicates a lower level of security culture. The numbers can be aggregated by individual areas/attributes of security system usability,

which becomes the basis for statements such as: "The Safeguard System of GIS is too risky, but only for such and such attributes/areas". To meet the thesis that the level of security culture of GIS must be measurable, it is required to characterise each element of the safeguard system of GIS with a set of risk factors together with their values, and then to show a measure of the level of security culture by a single numerical value, which makes it possible to compare and rank them directly.

Let`s introduce the following designations:

k – number of risk areas (categories) considered for the safeguard system of GIS

N_k – the number of risk factors falling into a given category

N_k^{MAX} – the maximum risk value assigned to the k-th category

R_v – the risk value for a factor belonging to a given category

w_k – weighting a category risk

w_{sr} – the average weight value calculated from the formula, $w_{sr} = \sum_v w_k \frac{R_v}{k}$

The level of risk culture, normalised to the interval [0,1]), can be determined as follows:

$$R_{n\_total} = \sum_x {}^{R_{zn\_x}}/_{k} \ , \ \text{where: } R_{zn\_x} = R_x \, {}^{w_x}/_{w_{sr}}, \ R_x = \sum_v {}^{R_v}/_{k * N_k}$$

The standardized values of a level of security culture and their interpretation are presented in Table 3.

Table 1. The standardized values of a level of security culture and their interpretation are presented by – Model

Value from – to	Weight
0.01 – 0.30	Strong security culture
0.31 – 0.60	Good security culture
0.61 – 1.00	Week security culture

Source: the in-house elaboration

Security Culture Grid

A very interesting instrument for measuring the level of safety culture is the Safety Culture Grid developed by G. Kirschstein and E. Werner-Keppner the Security Culture Grid (Kirschstein & Werner-Keppner, 2014). According to the authors, security culture is an indicator of the level of implementation and assimilation of security standards or security organization in a specific operating entity. With using the Security Culture Grid, the results of the "Management of Awareness" Analysis (BM Bewusst(Sein)-Managen) are summarized, and the "Management of Awareness" Ratio enables the outcomes to be compared with those of other actors. The Security Culture Grid of GIS shows the strengths and weaknesses of the cyber security culture of GIS and how solutions to further strengthen the security culture must be put in place. The graphical representation of the Security Culture Grid of GIS is shown in Figure 6.

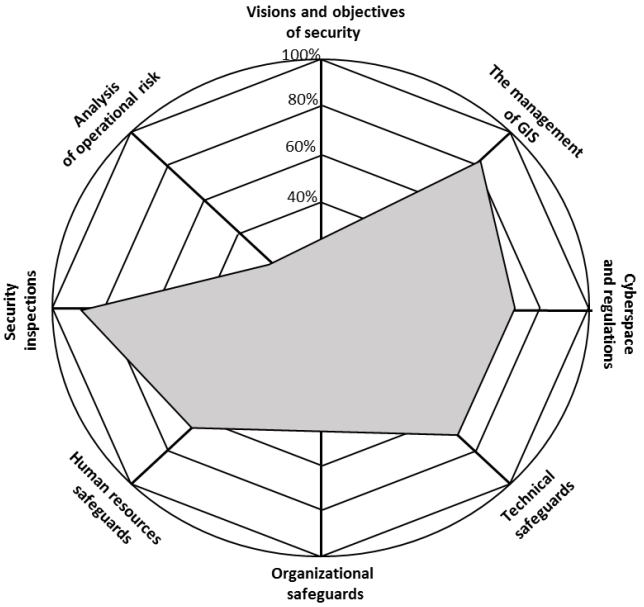

Fig. 6. Security Culture Grid of GIS
Source: the in-house elaboration

The grid takes the form of an octagon, at the poles of which are the factors/indicators that determine the level of security culture in cyber space of GIS. These are: security vision and objectives, operational risk analysis, security controls, personnel safeguards, organizational safeguards, GIS leadership, cyber space and regulation (Kirschstein & Werner-Keppner, 2014).

Conclusions

Properly implementing and maintaining a functioning organizational security system of GIS is not an easy task for GIS cyber space managers. This process requires an appropriate security culture. A culture of security requires that all responsibilities important to cyber security are carried out properly, on full alert, consciously and thoughtfully, with a full sense of responsibility – perfect procedures and practices are not enough. Measuring the level of security culture of GIS is closely related to assessing the effectiveness of safeguard features of GIS. Measuring the level of security culture is a function of the measures used (baseline and derived), the indicators, the measurement method and the specifics of the security system in question. The effectiveness of the measurement process depends on the activities carried out over a specified period of time covering the life cycle of the critical infrastructure of the GIS and ensuring compliance with the adopted methodology, ensuring consistency of measurement and addressing changes in the GIS computer system and its environment (regulations, requirements, measurement techniques).

The main objective of the paper was to systematize terms related to the concept of security culture of GIS, tools for shaping security culture and methods for measuring the level of security culture in cyber space of GIS. The primary purpose of measuring the level of security culture is to enable the construction of an effective safeguard and cyber

security management system of GIS by preparing such control decisions, also called directives or operating procedures, which will optimally direct/control the security state of critical infrastructure systems of GIS, in the sense of the adopted security indicator or criterion, e.g. the security culture level indicator.

An additional value of this document is the use of security culture metaphors that can enrich the process of measuring the level of security culture (make it more accurate). This is reflected in the methodology presented. The envisaged methodology has a theoretical background but is aimed at practitioners. The methodology is universal and can be used for all types of critical infrastructure systems of GIS as part of the cyber security management process. However, it is important that the selection of specific methods and techniques to support this measurement process depends on the situation (e.g. cyber threat system potential, realistic security system capabilities) and the capabilities of the analyzing GIS computer system.

The most important limitation of the methodology to measure the security culture of GIS is the theoretical nature of its foundations. Further empirical research (e.g. a case study) is therefore recommended, as well as a theoretical critique of the method.

The analysis of the state of the security culture of GIS should cover technical, organizational and human aspects. Assessing the state of the security culture of GIS in technical and organizational areas is a process that does not require designing dedicated solutions. The most difficult part of the security system is the human factor. Implicit views and beliefs have a significant impact on the level of security at work, yet are very difficult to identify and to quantify.

References

Abu Shawar B., Atwell E. (2007). Different measurements metrics to evaluate a chatbot system. In: Bridging the gap: academic and industrial research in dialog technologies, workshop proceedings, pp. 89–96. http://dl.acm.org/citation.cfm?id=1556341 (31.05.2021).

Cieślarczyk M. (2012). Societies and communities at the turn of the century – from the security of culture to the culture of security. 11th National Sociological Meeting, Rzeszów-Tyczyn.

Cieślarczyk M. (2010). Kultura bezpieczeństwa i obronności. Siedlce, p. 210.

Gabryelewicz I., Krupa P., Sadłowska-Wrzesińska J. (2017). Online measurement of work safety culture – statement of research. The 4th International Conference on Computing and Solutions in Manufacturing Engineering 2016 – CoSME'16, vol. 94. DOI: https://doi.org/10.1051/matecconf/20179406008.

Gaździcki J. (2010). Systemy informacji przestrzennej (*Spatial Information Systems*). Państwowe Przedsiębiorstwo Wydawnictw Kartograficznych im. Eugeniusza Romera.

Gwoździewicz S., Tomaszycki K. (ed.) (2017). Prawne i społeczne aspekty cyberbezpieczeństwa (*Legal and social aspects of cybersecurity*), Warszawa.

Kirschstein G., Werner-Keppner E. (2014). How to measure Security Culture? http://kirschstein.cz/pl/download/postergk-A4-pl.pdf [access: 06.01.2021].

Kowal E., Krupa P., Gabryelewicz I. (2015). The use of computer application in the analysis of safety culture firefighters – initial tests. In: M. Zachar, B. Falatová, Advances in Fire and Safety Engineering: Zborník Príspevkov z IV. Medzinárodnej Vedeckej Konferencie. Techická Univerzita, Zvolen.

Korzeniowski F. (2000). Zarządzanie bezpieczeństwem (*Safety management*), Kraków, p. 437.

Krupa P, Patalas-Maliszewska J., Gabryelewicz I. (2018). Metodyka badania poziomu kultury bezpieczeństwa w przedsiębiorstwach produkcyjnych – studium przypadku (*Methodology of testing the level of safety culture in manufacturing companies – a case study*). Zeszyty Naukowe. Organizacja i Zarządzanie, vol. 117, pp. 305–320, Politechnika Śląska.

Prauzner T. (2012). Technologia informacyjna – wybrane problemy społeczne (*Information technology – selected social problems*). In: W. Walat (ed.), Edukacja Technika-Informatyka. Wybrane problemy edukacji informatycznej i informacyjnej (*Education Technology – IT. Selected problems of IT and information education*), Rocznik Naukowy, no. 3.

Piwowarski J. (2010). Bezpieczeństwo jako stan oraz jako wartość (*Safety as a condition and as a value*). In: Bezpieczeństwo jako wartość (*Safety as a value*), Materiały z II Konferencji Naukowej Bezpieczeństwo jako wartość, 18 kwietnia 2010, Kraków.

Shaw A., Blewitt V. (1996). Telling tales: OHS and organizational culture. Journals of Occupational Health and Safety, vol. 12(2), pp. 185–191.

Sienkiewicz P. (2015). Ontologia cyberprzestrzeni (*Cyberspace ontology*). Zeszyty Naukowe WWSI, vol. 9, no. 13.

Stanik J., Kiedrowicz M. (2021). A Model for Measuring Risk Culture in the Information Society. 37th IBIMA Conference: 30–31 May 2021, Cordoba, Spain.

Stanik J., Protasowicki T. (2020). Cyberspace and Cybersecurity Models Based on Theory of Systems and Cybernetics. 36th IBIMA Conference: 4–5 November 2020, Granada, Spain.