VARSTVOSLOVJE, Journal of Criminal Justice and Security year 13 no. 2 pp. 222-239

The Nature of Security Culture in a Military Organization: a Case Study of the Slovenian Armed Forces

Denis Čaleta, Katja Rančigaj, Branko Lobnikar

Purpose:

The purpose of this research article is to define and explain the role of security culture as an important factor in the provision of effective preparedness of security organisation members for managing new types of security challenges, which are transnational, asymmetric and complex in form. It should be noted that, to a great extent, the internalisation of security awareness and the attitude towards security information depends on the organisational dynamics in an organisation. The article will complement theoretical findings with the analysis of the nature of security culture in a security (military) organisation, the priority of which is a high level of awareness of the effects of security culture and its integration in individual and organisational values.

Methods:

The article presents views of the Slovenian Armed Forces' (SAF) members on the perception of factors relevant for the operation of processes forming security culture. The research was carried out on a sample of SAF employees who use classified information in their work. Altogether 53 respondents participated in the survey. The security culture was measured with questions in the form of 31 statements. The respondents answered these statements with the help of a five-level scale. The Cronbach's alpha coefficient for the listed statements was 0.932. Finally, the nature of security culture was established with the help of a factor analysis.

Findings:

A factor analysis, carried out at the beginning of the analysis, helped establish six factors of security culture which enabled us to explain 71.99 percent of the variance. The identified factors intended for explaining security culture in the context of a military organisation are as follows: personnel requirements for management of classified information, competence for maintenance of security culture, attitude towards the protection of classified information, procedures for ensuring protection of classified information, recording and elimination of violations in the protection of classified information and organisational measures for management of classified information. The results of the survey carried out among the SAF employees demonstrated that the respondents estimated marked

all identified security culture sets of contents above average, with marks ranging between 3 and 4 in all statements.

Research limitations/implications:

The survey covered those SAF members who use classified information in their work. Hence the results of the survey are primarily applicable to the military environment and could not be generalized for other security organisations.

Practical implications:

The results of the survey can be directly applied to the management of processes for the protection and management of classified information in the SAF. Furthermore, they also indicate the application of the theoretical understanding of security culture's significance to the success of security organizations' performance.

Originality/Value:

The survey introduces an original approach to the measurement of security culture in security organisations. It can serve as a valuable basis for further research on the interaction of security culture with other factors in security organisations, such as for instance organisational culture. Practicians of criminal justice and security, military science and other similar scientific disciplines can also find this article useful in their further study of standpoints and attitudes of security organisations' members about their role in the processes of establishing an appropriate security culture, as a precondition for effective management of new challenges and threats that we witness in the contemporary security environment.

UDC: 355/359(497.4)

Keywords: security culture, armed forces, classified information, Slovenia

Narava varnostne kulture v vojaški organizaciji: primer Slovenske vojske

Namen:

Varnostna kultura je dejavnik, ki pomembno vpliva na pripravljenost zaposlenih v varnostni organizaciji, da se učinkovito soočajo z asimetrični, transnacionalnimi in kompleksnimi varnostnimi izzivi v sodobni družbi. Organizacijska dinamika je namreč tisti dejavnik, ki pomembno vpliva na procese ponotranjenja pravil varnostnega vedenja, in preko tega tudi na vedenjske odzive zaposlenih, ko se srečujejo z upravljanjem varnostnih podatkov. Avtorji v prispevku teoretično opredelitev področja nadgradijo z analizo podatkov o naravi varnostne kulture v varnostni (vojaški) organizaciji.

Metode:

V prispevku so predstavljeni rezultati raziskave, izvedene na vzorcu pripadnikov Slovenske vojske, kjer avtorji analizirajo njihovo percepcijo pomembnih faktorjev za tvorjenje učinkovite varnostne kulture znotraj vojaške organizacije. V vzorec so bili vključeni tisti pripadniki Slovenske vojske, ki pri svojem delu uporabljajo tajne podatke (N=53). Varnostno kulturo so avtorji merili s pomočjo vprašalnika z 31 trditvami na petstopenjski lestvici Likertovega tipa. Cronbach alfa

koeficient za uporabljeno lestvico je bil 0.932. Vsebina in narava varnostne kulture v vojaški organizaciji je bila analizirana s pomočjo faktorske analize.

Ugotovitve:

S pomočjo faktorske analize je bilo ugotovljenih šest skupin/faktorjev varnostne kulture v vojaški organizaciji, s pomočjo katerih so avtorji pojasnili 71.99 odstotkov celotne variance. Faktorji, s pomočjo katerih pojasnjujejo naravo varnostne kulture, so naslednji: na posameznika vezani pogoji za upravljanje s tajnimi podatki, kompetence za vzdrževanje varnostne kulture, odnos do varovanja tajnih podatkov, postopki za zagotavljanje varnosti tajnih podatkov, evidentiranje in odpravljanje kršitev v postopku varovanja tajnih podatkov in organizacijski postopki za upravljanje področja varovanja tajnih podatkov. Rezultati raziskave kažejo nadpovprečne vrednosti pri analiziranih vsebinah, saj so udeleženci svoje odgovore označevali v veliki večini z vrednostmi 3 ali 4.

Omejitve:

Raziskava je vključevala zgolj tiste pripadnike Slovenske vojske, ki pri svojem delu uporabljajo tajne podatke. Zato so ugotovitve uporabne predvsem v okviru analize v vojaški organizaciji in niso primerne za posploševanje na druge varnostne organizacije.

Praktična uporabnost:

Rezultate raziskave je mogoče neposredno uporabiti v procesu upravljanja področja varovanja tajnih podatkov v okviru Slovenske vojske. Poleg tega pa prispevek krepi zavedanje po potrebi razumevanja širšega teoretičnega okvirja razumevanja varnostne kulture in njenega vpliva na organizacijsko učinkovitost.

Izvirnost:

Raziskava predstavlja izviren pristop merjenja varnostne kulture v varnostnih organizacijah. Kot takšna lahko služi kot pomemben izvor pri nadaljnjem raziskovanju tega področja, še posebej pri proučevanju povezanosti dejavnikov varnostne kulture z drugimi pomembnimi organizacijskimi procesi, kot je na primer organizacijska kultura. Praktiki in raziskovalci s področja varstvoslovnih, vojaških in obramboslovnih ved lahko rezultate raziskave uporabijo tudi pri nadaljnjem proučevanju pomena mnenj zaposlenih v varnostnih organizacijah pri vzpostavljanju varnostne kulture.

UDK: 355/359(497.4)

Ključne besede: varnostna kultura, vojska, tajni podatki, Slovenija

1 INTRODUCTION

Gambetta (Tan & Tan, 2000) defined trust in an organization as a global assessment of the organisation's reliability in the eyes of its member. According to the author, trust in an organisation includes a member's belief that the organisation will carry out activities beneficial to the member or at least not in contradiction with his interests. In this context we should also mention that Gambetta starts from Robins' (Kramer, 1999: 570; Perry & Mankin, 2004: 277) general definition of trust, which says that trust "includes individual's expectations, presumptions and beliefs

regarding the possibility that someone else's future actions will be beneficial for the individual or, at the least, will not impair his interests". In addition to justice present in an organisation, trust is linked with the perception of the support the organisation offers to the employees which reflects the general perception of employees on the organisation's appreciation for their contributions (Eisenberger in Tan & Tan, 2000; Huntington in Tan & Tan, 2000). The perception of the support of an organisation is a part of an arrangement on mutual exchange between the employee and the organisation. Authors differ greatly in their opinion of the influence that trust has on the operation of an organisation. However, the majority of authors believe that trust has positive effects on the organisation. The common standpoint of all authors is reflected in the observation that trust is a kind of a mitigatory mechanism whose role is to facilitate relations between the players and diminish control-related transaction costs (Cummings & Bromiley in Bijlsma & Koopman, 2003: 550; Curral & Judge in Bijlsma & Koopman, 2003: 550; Smith & Barclay in Bijlsma & Koopman, 2003: 550). Positive views of organisation members are closely linked to their trust in the organisation. A high level of organisational trust and a positive orientation of member's standpoints regarding the organisation are very closely connected to more flexible organisation forms and structures, strategic alliances, effective crisis management, lower costs of legal procedures, innovation of products and economic performance (Ellis & Shockley-Zabalak, 2001: 384). The stated factors and effects can be supplemented by the loyalty to an organisation, work satisfaction, satisfaction with superiors, group affiliation and a high level of cooperation (Bijlsma & Koopman, 2003: 547).

The organisational structure undoubtedly forms a framework, within which the standpoints of its members play an important role. Convictions and expectations create norms that strongly shape the behaviour of individuals in a group or an organisation (Dabić & Potočan, 2007). Martin (2002: 57) defined the organisational culture as a pattern of shared convictions and values giving importance to members of an organisation and ensuring them rules of conduct in an organisation. Možina et al. (1994: 145-146), Mihalič (2004) and also Brown (1998) defined this process as a way of common thinking and operating in a group, which is something that the new members have to learn in order to survive and be part of this organisation. The organisational culture, including its standpoints and their influence on the effectiveness of an organisation, is preserved and developed in the process of learning and socialisation. All listed theoretic cognitions, applicable primarily in business organisational environment, can definitely be transferred to and examined in the environments of the national security system organisation which have a special role in the protection of classified information.

The human being is a central and a crucial link in the system of classified information protection. As part of the organisational culture, security culture is an important segment in the establishment of effective mechanisms in environments in which the employees protect and process classified information. Security awareness of the employees presents that segment in which the management of an effective organisation particularly endeavours to increase the mentioned level of awareness through various approaches. These approaches are reflected in different forms of conscious and unconscious influences on the actions and attitude of

employees. Furthermore, security culture could also be defined as the awareness of the members of a certain organisation about their rights, obligations and their application. Those belonging to a specific security culture are aware of how their knowledge influences security and are willing to educate those members of the organisation who do not comply with the patterns of security culture by setting an example and offering advice (Čaleta, 2008).

We could conclude that security awareness overgrows into security culture in that moment when a group as a whole starts to perceive security violations as socially and morally unacceptable to the group. Another important factor influencing security culture, besides continuing education, is the personal example, which is transferred to other members of that organisation by the management. We should, however, be aware that each organisation has a unique form of security culture, which is characteristic only for the form and the operation of that same organisation. Security culture as such can be either unifying or destructive and can appear in structured or unstructured forms. It presents an entire spectrum of security habits and behaviours that are established in a certain social group. Security culture thus provides basic foundation for the prevention or reduction of deviant security phenomena. As a social process of assembling and protecting its members, security culture appears in those structures where the feeling of threat within the group is most pronounced, e.g. in terrorist groups and criminal or other organisations, the operation of which is based on illegal activities. Due to the feeling of constant threat from security authorities, security culture is especially expressed in these structures. In the time of globalisation processes, the need for integration of adequate security culture patterns can be also perceived in commercial entities which dedicate increasingly more system and organisational measures to this phenomenon (Čaleta, 2004a, 2004b).

In its wider sense, security can be an integral part of the overall process that takes place in an organisation. It is defined already in the phase of identifying organisational processes by means of projects or it can be considered as an isolated process that is applied or integrated only in individual phases of the organisation's operation. If the management of an organisation does not consider the significance and the effects of security culture as one of its priorities, it is practically impossible to expect that the members of such organisation will adequately internalise the patterns of security awareness and as a result perceive the security of classified information as important. We could assess that the most important thing is to coordinate the strategy of protecting classified information with the strategy of the operation of an organisation or its mission. Risk assessments must be clearly defined for the entire organisation and its individual parts. Both the management and the employees of an organisation, particularly those who have an important role in the protection of classified information, must have a thorough knowledge of risk assessments. By increasing the level of awareness about the possibility of various threats to the organisation, the importance of security and the protection of classified information are indirectly enhanced. By no means should we neglect the importance of the middle management level which has a visible role in the increasing of security culture of the employees in an organisation. The top management must ensure the process of continued informing about security policy regarding

the protection of classified information and all deviant phenomena and measures for their elimination. Particular consideration should be placed on policy, which ensures a proactive approach towards the prevention of the occurrence of reasons for deviant acts concerning protection of various forms of classified information. It is not only the approach to informing about the events that present a threat to security that is important. We also have to ensure that adequate knowledge and experiences connected to these events will be communicated through the process of lessons learned[1].

A proper transmission of information in the form that is easily comprehensible, understandable and acceptable for the employees of an organisation is a crucial factor for the individual's perception of relevant security-related phenomena. The educational process requires the use of various statistical and financial models for all levels of employees. These models clearly demonstrate the relation between the invested means that are necessary for preventive measures used in ensuring confidentiality of classified information, and the financial risk assessment or consequences of deviant events connected to the loss of certain types of information previously defined as classified. The financial aspect and the financial assessment is, particularly for the management staff, always an effective means of understanding the importance of security measures in a wider sense and the protection of classified information in the narrower sense.[2] The building of a security organisation and security culture can only be successful, if the model is applied from the highest to the lowest levels of the organisation. However, the aspect of or the approach to delegating responsibility for the effective establishment of a security organisation and awareness to lower levels of the organisation is not effective and is reflected in negative effects on the entire system of protecting classified information. This reaffirms the fact that the top management has to prepare foundations for the establishment of security culture in an organisation by setting an example to others. If we apply these finding to the national security of the Republic of Slovenia, it is safe to conclude that behaviour patterns of elected representatives are important for successful enhancement of security awareness of the citizens, mainly those in charge of protecting classified information. With their actions and personal example concerning the protection of classified information, these representatives influence the perception of the need for adequacy of protection and for awareness of the importance of this area. Current activities and affairs relating to unauthorised alienation of classified information, which involve public figures, are far from positive in the eyes of citizens and send them a message about the necessity for adequate protection of classified information (Spence, 2007).

1 *The expression »lessons learned« means a process which has gained great importance in modern organisation sciences, for it integrates the existing knowledge, resulting in a form of experiential patterns integrated in future operation of the organisation and the individual.*

2 *In 2004, the Global Information Security Survey, which examined the assessment of damage in a company due to deviant events connected to security of information, was carried-out among European companies. The responses were as follows: 22 % have assessed the damage in the range up to $10,000, 11 % assessed the damage from $10,000 to $100,000, as much as 46 % could not assess the costs of such actions, while 21 % did not want to answer the question (Briggs & Edwards 2006: 45).*

In order to coordinate effective approaches towards enhancement of security culture in the protection of classified information, it is required to carry out all necessary processes for measuring and assessing the current level of security culture in the examined environments. These assessments can serve as a basis for further planning of organisational activities leading to a constant growth of awareness about the importance of security culture. It is important to observe the process of security culture as a long-term and not only as a short-term process. Today's circumstances in the global environment require coordinated operation of an individual organisation, the structure of which is intertwined with the process of security culture of individuals, whose activities are in line with security objectives. To be able to monitor the current situation, constant assessment of the effectiveness of fulfilling security demands and requirements is very important. Nowadays, various technological measures enable metric assessment of the attempts or the execution of deviant and disputable acts in security terms. A reliable application of surveillance mechanisms for measuring security culture requires a detailed prior knowledge of the structure and dynamics of an individual organisation. The performed analyses[3] indicate that the employees present a greater risk for the protection of various types of classified information than the threats outside the organisation system. We are rightfully concerned by this fact, which additionally increases the importance of security culture. Establishing adequate programmes of security awareness and emphasising procedures formed in the process of learning from experience and applying good practice, are logical activities, which must necessarily be followed by the development of adequate metric tools for the verification and acquisition of feedback information on the effectiveness of these activities. The training process is highly important for the development of security culture and can thus be submitted to certain procedures for measuring its effectiveness. Information acquired by the management through measurement of various process stages serve as a basis for corrective measures that are required for the attainment of the desired security culture in their organisation. The management of the organisation must be aware of the fact that metric information, acquired only in one area, can be deceiving and do not reflect the actual state in security culture. It is therefore necessary to establish an integral metric process, which effectively assesses the condition on various fields, establishes a realistic image of the state of security culture at the employees of an individual organisation and offers an adequate basis for implementing certain improvements. The metric model must contain a series of validation measures, achieved with the help of security technologies, processes and assessment of the employees' behaviour. Throughout the process of monitoring and adapting security awareness of employees, it is very important to collect and analytically process different information that is interesting from the security aspect and can be acquired through different surveys or from the already existent databases. Such analyses are used for the preparation of progressive forms

3 *In 2006, the Computer Security Institute (CSI) and the Federal Bureau of Investigation (FBI) carried out an inspection among the CSI members. The results showed that in 2005, over 30 % of larger companies participating in the inspection, estimated that the reason for at least half of the damage in the form of information confidentiality violation was caused by threats inside the system. Federal Bureau of Investigation, available at http://www.fbi (24 September 2007).*

of education and training for increasing security culture. Through these forms of education, the management directs the employees in the desired direction, striving to increase security culture. The training process, more precisely the information on the number of trainings and the participation of employees, must be constantly monitored. In connection with the acts that are contentious from the security aspect, this information offers an effective basis for the assessment of suitability of measures that the management implements in the area of education with a view to increase security culture. Metric tools must be adjusted in such a way that the results of the analysis are made accessible in adequate graphic, tabular and other forms. They should provide the management with access to or warning about the fields where additional activities for the maintenance or enhancement of the level of security awareness and security culture at the employees have to be carried out (Čaleta, 2004a, 2004b).

Security culture is of great importance in ensuring an adequate attitude of the members belonging to an individual organisation and not least an adequate attitude of society in its wider sense towards the protection of security. Lately, increasingly more attention is dedicated to the mentioned phenomenon, both in systemic and social sense. The responsibility for the development of security culture in individual members and organisations as a whole is dispersed on different management and administration levels of these organisations. Education and the knowledge management process have a very important role in the increasing of the level of security culture and the level of awareness regarding the need for effective protection of classified information. Further research of the models for measuring security culture level is essential for the acquisition of effective tools, which will help the management of an individual organisation to adequately evaluate and plan corrective measures for a higher level of security awareness (Čaleta, 2008).

Public authorities and in particular the elected representatives of the nation play their own part in the area in question. By setting an example they strongly influence the integral attitude of citizens towards the protection of classified information process on both conscious and subconscious levels. Legislation determining regulatory arrangements for the protection of classified information must ensure adequate flexibility and responsiveness to all changes occurring in relation to the right to access publicly accessible information and protect various types of classified information.

2 DESCRIPTION OF THE METHOD USED, THE QUESTIONNAIRE AND THE SAMPLE

In October and November 2008, a survey was carried out for the SAF employees who have access to classified information. Altogether 53 respondents participated in the survey, out of which 10 % were females. The average age of respondents was 41.95 years (from minimum 22 to maximum 55 years), with 12.98 years of service on average. On average they occupied their current work post for 3.18 years. The majority of respondents (44.9 %) had higher or university education, 30.6 % had high-school education, 14.3 % had postgraduate education, 8.2 % of the

respondents stated that they had short-term higher education. Three quarters of respondents had the right to access information of confidential nature or classified as secret or top secret.

Security culture was measured with questions in the form of 31 statements. The respondents answered the statements with the help of a five-level scale, at which 1 indicated that they did not agree with the statement and 5 indicated that they strongly agreed with the statement. Cronbach's alpha coefficient for the listed statements is 0.932, which means that the questionnaire on security culture is internally consistent. For an easier analysis or reduction of data we carried out a factor analysis. We excluded five statements out of that analysis, since they could not be placed under any individual factor. Therefore we included 26 statements in the final analysis. The KMO test for these 26 statements was 0.738.

3 RESULTS

At the beginning of the analysis we carried out a factor analysis with which we acquired six factors, helping us to explain 71.99 percent of the variance. More precise information on the factor analysis is presented in Table 1 below.

Table 1: Distribution of individual factors and jointly explained variance

Component	Initial Eigenvalues	
	Total	% of Variance
1	10.217	39.298
2	2.613	10.051
3	1.915	7.365
4	1.532	5.890
5	1.265	4.867
6	1.177	4.526

Distribution of statements used for measuring security culture is presented in Table 2 below.

Table 2: Distribution of statements used for measuring security culture

Statements	Factors					
	1	2	3	4	5	6
The number of employees in our unit and their competence suffice for successful protection of classified information.	.875					
Our organisational unit produced a plan for protection of classified information which is adapted to specific operation of our organisational unit.	.769					

The flow of information provided in our unit ensures that the employees are properly informed of the protection of classified information.	.747					
In our unit appropriate division of tasks and responsibilities for protection of classified information is ensured.	.708					
Our unit envisages precise measures that are to be undertaken in the event of non-compliance with regulations regarding the protection of classified information.	.697					
Everyone in our unit knows precisely who is in charge of the protection of classified information.	.687					
There is a set procedure in our unit which ensures that all employees are familiar with the provisions regarding the protection of classified information.	.657					
In the interest of increasing security culture, it is important to organise periodic training in our organisation.		.822				
It is necessary to educate the employees in our organisation about security culture.		.793				
The management of our organisation has appropriate attitude towards security culture.			-.897			
The employees of our organisation have appropriate attitude towards the protection of classified information.			-.782			
With its behaviour the management sets an appropriate example for the employees in reference to the protection of classified information.			-.761			
In my opinion the newly employed workers in our organisation have adequate security awareness.			-.734			
In security terms the classified information management in our organisation is suitable.			-.697			
The management in our organisation responds to the initiatives of subordinates to improve the protection of classified information in due time.				.731		
My co-workers morally condemn the abuse of classified information.				.688		
The management in our unit adequately responds to the findings of internal control regarding the protection of classified information.				.602		
Information and communication systems in our organisation are appropriately adapted to the required standards for the protection of classified information.				.577		

Our unit has a systematic method for recording and monitoring security violations.					-.912	
The control over the handling of secret or confidential information in our organisation is adequate.					-.792	
In our unit the verification of effectiveness and successfulness of the operation of the system for the protection of classified information is carried out in a proper manner.					-.738	
The management of our unit actually carries out measures that are to be undertaken in the event of non-compliance with the provisions regarding the protection of classified information.					-.716	
All employees in our unit are familiar with the risks identified in relation to the protection of classified information in their organisational unit.						.830
In our unit, the organisational structure, responsibilities and competences in the field of classified information are clearly defined and described.						.700
In our unit, risks related to protection of classified information are well defined.						.672
The employees in our organisation have the possibility for appropriate reporting of any irregularities and problems in the protection of classified information.						.617

Rotation method: Oblimin / Kaiser Normalization.

Factor no. 1 which explains 39.29 percent of the joint variance refers to wider personnel requirements that are necessary to ensure the protection of classified information, since it includes statements such as "The number of employees in our unit and their competence suffice for successful protection of classified information.", "Our organisational unit produced a plan for protection of classified information which is adapted to specific operation of our operational unit.", "The flow of information provided in our unit ensures that the employees are properly informed of the protection of classified information."… Hence this factor was named "***Personnel requirements for the management of classified information***".

The second factor, used for explaining additional 10 percent of the variance, refers to acquiring competences for the development of security culture, since the two statements classified under it are: "In the interest of increasing security culture it is important to organise periodic training in our organisation." and "It is necessary to educate the employees in our organisation about security culture.". Therefore the second factor was named "***Qualification for maintenance of security culture***".

The third factor which additionally explains 7.3 percent of the joint variance in its content refers to the question of attitude towards the protection of classified information, since it includes the following statements: "The management of our

organisation has appropriate attitude towards security culture.", "The employees of our organisation have appropriate attitude towards the protection of classified information.", "With its behaviour the management sets an appropriate example for the employees in reference to the protection of classified information." and "In my opinion the newly employed workers in our organisation possess adequate security awareness."… The third factor was named "***Attitude towards the protection of classified information***".

In terms of its contents, the fourth factor (explains 5.8 percent of the joint variance) refers to the provision of conditions for the protection of classified information, since the following statements were listed under this factor: "The management in our organisation responds to the initiatives of subordinates to improve the protection of classified information in due time.", "My co-workers morally condemn the abuse of classified information.", "The management in our unit adequately responds to the findings of internal control regarding the protection of classified information." and "Information and communication systems in our organisation are appropriately adapted to the required standards for the protection of classified information.". This factor was therefore named "***Procedures for the provision of protection of classified information".***

The fifth factor (explains additional 4.8 percent of the variance) addresses the question of recording violations and implementing control over procedures for the protection of classified information. The following statements were classified under this factor: "Our unit has a systematic method for recording and monitoring security violations.", "The control over the handling of secret or confidential information in our organisation is adequate.", "In our unit the verification of effectiveness and successfulness of the operation of the system for the protection of classified information is carried out in a proper manner." and "The management of our unit actually carries out measures that are to be undertaken in the event of non-compliance with the provisions regarding the protection of classified information.". This factor was named "***Recording and elimination of violations in the protection of classified information***".

In the last, sixth factor, which was used for explaining additional 4.5 percent of the joint variance, the following statements were classified: "All employees in our unit are familiar with the risks identified in relation to the protection of classified information in their organisational unit.", "In our unit, the organisational structure, responsibilities and competences in the field of classified information are clearly defined and described.", "In our unit, risks related to protection of classified information are well defined.", and "The employees in our organisation have the possibility for appropriate reporting of possible irregularities and problems in the protection of classified information.". This factor was named "***Organisational measures for management of classified information***".

Further on are presented the results of descriptive statistics joined under individual factors.

Table 3: Contents referring to personnel requirements for the management of classified information

"Personnel requirements for the management of classified information"		
Statements	Mean	Standard deviation
The number of employees in our unit and their competence suffice for successful protection of classified information.	3.49	1.067
Our organisational unit produced a plan for protection of classified information which is adapted to specific operation of our operational unit.	3.42	1.082
The flow of information provided in our unit ensures that the employees are properly informed of the protection of classified information.	3.31	.919
In our unit appropriate division of tasks and responsibilities for protection of classified information is ensured.	3.42	1.016
Our unit envisages precise measures that are to be undertaken in the event of non-compliance with regulations regarding the protection of classified information.	3.22	1.045
Everyone in our unit knows precisely who is in charge of the protection of classified information.	3.40	1.159
There is a set procedure in our unit which ensures that all employees are familiar with the provisions regarding the protection of classified information.	3.42	1.082

The results presented in the table show that the respondents marked all statements classified in the set that refers to personnel requirements which are necessary for a successful and effective management of classified information with a very high average mark. As far as the number and the qualification of personnel in charge of protecting classified information are concerned, more than two thirds believe that this number and their qualification suffice. Over 92 percent believe that all employees in their unit are precisely informed of the procedures for the protection of classified information. On the other hand, only 35 percent are convinced that the employees in their unit know what is the procedure undertaken in the event of non-compliance of regulations for the protection of classified information.

Table 4: Assessment of the importance of qualification for maintaining security culture

"Qualification for maintenance of security culture"		
Statements	Mean	Standard deviation
In the interest of increasing security culture it is important to organise periodic training in our organisation.	4.11	.891
It is necessary to educate the employees in our organisation about security culture.	4.26	.880

The above table clearly demonstrates that the respondents, only those who are familiar with the management of classified information, are convinced that the key to maintaining a high level of security culture lies in quality training and education of employees. Hence the information that as much as 79 percent strongly agree that

education in security culture is in the eyes of employees an important factor for the maintenance of security culture, comes as no surprise.

"Attitude towards the protection of classified information"		
Statements	Mean	Standard deviation
The management of our organisation has appropriate attitude towards security culture.	3.28	.968
The employees of our organisation have appropriate attitude towards the protection of classified information.	3.36	.901
With its behaviour the management sets an appropriate example for the employees in reference to the protection of classified information.	3.15	.937
In my opinion the newly employed workers in our organisation possess adequate security awareness.	2.96	.980

Table 5: Assessment of the employees' and the organisations' attitude towards the protection of classified information

In assessing the attitude towards the protection of classified information, we can establish that much could still be done in the area of informing the newly employed of security, since less than one third of the respondents believe that the new employees have been thoroughly informed of the rules and procedures for the protection of classified information.

"Procedures for the provision of protection of classified information"		
Statements	Mean	Standard deviation
The management in our organisation responds to the initiatives of subordinates to improve the protection of classified information in due time.	3.04	.894
My co-workers morally condemn the abuse of classified information.	3.42	.936
The management in our unit adequately responds to the findings of internal control regarding the protection of classified information.	3.36	.942
Information and communication systems in our organisation are appropriately adapted to the required standards for the protection of classified information.	3.29	1.073

Table 6: Assessment of procedures for the provision of protection of classified information

The results presented in Table 6 demonstrate the respondents' conviction that their co-workers internalised the values of protecting classified in information and their inclination to morally condemn the abuse of such information. This is particularly important form the aspect of security culture, since it is the internalised and not the forced norms that contribute to a more consistent behaviour.

Table 7: Assessment of procedures for effective recording of violations and their elimination

"Recording and elimination of violations in the protection of classified information"		
Statements	Mean	Standard deviation
Our unit has a systematic method for recording and monitoring security violations.	3.00	1.048
The control over the handling of secret or confidential information in our organisation is adequate.	3.60	.995
In our unit the verification of effectiveness and successfulness of the operation of the system for the protection of classified information is carried out in a proper manner.	3.14	.917
The management of our unit actually carries-out measures that are to be undertaken in the event of non-compliance with the provisions regarding the protection of classified information.	3.04	.907

The field of recording and eliminating security violations was likewise assessed as satisfactory, since all average marks at individual statements equal to or are higher than 3. It is nonetheless true that as much as one third of respondents did not agree with the first statement in Table 7. This also explains the high standard deviation at an average high value.

Table 8: Assessment of organisational measures for effective management of classified information

"Organisational measures for management of classified information"		
Statements	Mean	Standard deviation
All employees in our unit are familiar with the risks identified in relation to the protection of classified information in their organisational unit.	3.42	1.109
In our unit, the organisational structure, responsibilities and competences in the field of classified information are clearly defined and described.	3.58	.997
In our unit, risks related to protection of classified information are well defined.	3.25	.860
The employees in our organisation have the possibility for appropriate reporting of possible irregularities and problems in the protection of classified information.	3.25	1.046

According to the respondents' belief, the minimum essential measures for the protection of classified information are established at both individual and organisational levels. For this reason the respondents evaluated very highly the risk assessment, the communication procedures and the type of organisational design with the help of which are presented the procedures for the protection of classified information.

Table 9 depicts the results of a correlation analysis between individual factors which were used to define security culture in the analysed organisation – the Slovenian Armed Forces. We can establish that individual factors rarely correlate

with each other in a significant way, which means that each of the described factors can be defined as relatively independent in the security structure of the Slovenian Armed Forces. We have identified a positive and statistically significant connection only between the attitude towards the protection of classified information and the assessment of efficiency together with the elimination of violations in the management of classified information. Those respondents that estimated the attitude towards protection as good or even better also reported that the system of recording and taking measures in case of mistakes and abuses is, to their belief, a good system. Furthermore, what is interesting is a negative and statistically significant correlation between the assessment of personnel requirements for the management of classified information and the procedures for recording violations. It is interesting that those respondents that gave a high mark to personnel requirements intended to ensure effectiveness and efficiency of the Slovenian Armed Forces in the field of security culture, gave a lower mark to the readiness for recording violations. The result could conditionally be explained with the help of the so-called code of silence – in environments in which co-workers are strongly connected with each other there is less willingness to report of violations committed by their co-workers.

Factors		1	2	3	4	5	6
1 "Personnel requirements for management of classified information"	r	1.000					
	p						
2 "Qualification for maintenance of security culture"	r	-.012	1.000				
	p	.935					
3 "Attitude towards the protection of classified information"	r	-.247	-.067	1.000			
	p	.084	.643				
4 "Procedures for the provision of the protection of classified information"	r	.232	.050	-.226	1.000		
	p	.105	.731	.114			
5 "Recording and elimination of violations in the protection of classified information"	r	-.346*	-.161	.362**	-.258	1.000	
	p	.014	.266	.010	.070		
6 "Organisational measures for management of classified information"	r	.291*	.023	-.191	.136	-.258	1.000
	p	.041	.873	.185	.346	.070	

Table 9: Correlation analysis between individual factors

4 DISCUSSION AND CONCLUSIONS

The report presents the deliverables of the research carried out on a sample of the Slovenian Armed Forces' employees who deal with various types of classified information in their work. In the light of security culture we established that the managers of this system must pay special consideration to the following six sets of contents that are relatively independent:

a) Personnel requirements for the management of classified information;

b) Qualification for maintenance of security culture;
c) Attitude towards the protection of classified information;
d) Procedures for the provision of the protection of classified information;
e) Recording and elimination of violations in the protection of classified information, and
f) Organisational measures for management of classified information.

However, on the basis of the results, it can be established that the respondents estimated very high all sets of contents regarding security culture in the SAF, defined in the paragraph above, with the marks of the statements ranging between 3 and 4. One critical observation that could be identified on the basis of the results is the dispersion of answers – despite the good average assessment some respondents were very critical of certain areas of protection of classified information. In such a sensitive area as security culture, this is a serious indication that certain measures for the strengthening of this culture must be taken. The results offer guidelines on how to achieve this. According to the respondents, security culture can be improved and strengthened by means of education and training. Of course, it is necessary to realize that education is not the only way to achieve a higher level of security culture. A numerous factors have influence in these processes. Role of management of the organization has in this respect perhaps the most important role. Organizational leaders through their personal examples and attitude towards the importance and enforcement of security set the minimum standards and understanding of the importance of safeguarding the classified information.

Throughout the study a high percentage of respondents answered that they do not approve misuse of classified information. This is certainly an important positive indicator in a process of strengthening the existing culture. However, it may turn quickly enough into a form of passivity and conscious violations of established rules if the organization faces a passive attitude of management and poor control mechanisms in the events of security infraction.

Working environment, as another important factor, should be considered separately through the survey as well. It is necessary to highlight the working environment and conditions that affect employee's satisfaction with the organization and its processes. Disgruntled and unmotivated members of the organization are definitely less receptive towards the intentional and unintentional security violations.

REFERENCES

Bijlsma, K., & Koopman, P. (2003). Introduction – Trust within Organizations. *Personel Review*, *32*(5), 543-555.

Briggs, R., & Edwards, C. (2006). *The Business of Resilience – Corporate Security for the 21st Century*. London: Demos.

Brown, A. (1998). *Organizational Culture*. London: Financial Times Pitman Publishing.

Čaleta, D. (2004a). *Sistem varovanja tajnih podatkov* (MA thesis). Ljubljana: FPDEŠ.

Čaleta, D. (2004b). Dileme varovanja tajnosti v demokratični družbi. *Dignitas*, (21/22), 164-178.

Čaleta, D. (2008). Varovanje tajnih podatkov v demokratični družbi. *Dignitas*, (37/38), 249-271.

Dabić, M., & Potočan, V. (2007). Organizacijska kultura v sodobnih organizacijah. In V. Rajkovič (Ed.), *Ustvarjalna organizacija* (pp. 391-398). Kranj: Moderna organizacija.

Ellis, K., & Shockley-Zabalak, P. (2001). The Relationship to Satisfaction, Perceived Organizational Effectiveness and Information Receiving. *Communication Quarterly*, *49*(4), 382-398.

Kramer, R. M. (1999). Trust and Distrust in Organizations: Emerging Perspectives, Enduring Question. *Annual Review of Psychology*, (50), 569-598.

Martin, J. (2002). *Organizational Culture: Mapping the Terrain*. California: Sage.

Mihalič, R. (2004). Dimenzije upravljanja organizacijske kulture in klime. *Znanstveno delo podiplomskih študentov v Sloveniji* (pp. 381-389). Ljubljana: Društvo mladih raziskovalcev Slovenije – združenje podiplomskih študentov.

Možina, S. et al. (1994). *Osnove vodenja*. Ljubljana: Ekonomska fakulteta.

Perry, R. W., & Mankin, L. D. (2004) Understanding Employee Trust in Management: Conceptual Clarification and Correlates. *Public Personnel Management*, *33*(3), 277-290.

Spence, K. (2007). Globalizing Security, Securing Globalization? Privatization, Commodification and the New Terrorist Threat. In O. Nikbay, & S. Hancerli (Eds.), *Understanding and Responding to the Terrorism Phenomenon: A Multi-Dimensional Perspective*, (pp. 417–430). Amsterdam: IOS Press and NATO Public Diplomacy Division.

Tan, H., & Tan, C. (2000) Toward the Differentiation of Trust in Supervisor and Trust in Organization. *Genetic, Social and General Psychology Monographs*, *126*(2), 241-261.

About the Authors:

Dr. Denis Čaleta, Assistant Professor of Security Organization Management, Ministry of Defence, Republic of Slovenia.

Katja Rančigaj, MA, Lecturer of Policing and Management of Security Organizations, Faculty of Criminal Justice and Security, University of Maribor, Slovenia.

Dr. Branko Lobnikar, Associate Professor of Policing and Management of Security Organizations, Faculty of Criminal Justice and Security, University of Maribor, Slovenia.