UDC 65.012.3:681.518:331.45
DOI: 10.7562/SE2012.2.03.09
Original article
www.safety.ni.ac.rs

BUILDING MANAGEMENT IN THE INTELLIGENCE AND SECURITY COMMUNICATION NETWORK

MAID PAJEVIĆ [1]
ARMIN KRŽALIĆ [2]

[1] Agency for Education and Training
of Police Personnel of
Bosnia and Herzegovina,
Mostar, Bosna i Hercegovin;
College "Logos Center" Mostar,
Department of Security,
Mostar, BiH.
[2] College "Logos Center" Mostar,
Department of Security,
Mostar, BiH

[1]*maid.pajevic@aeptm.gov.ba*
[2] *armin.krzalic@gmail.com*

Abstract: *Security and intelligence services, at present time, are more exposed to public criticism due to terrorist acts which, as a consequence, had large number of people being killed and material damage being caused. Security and intelligence services have been observed trough the following: operative fails, organizational disadvantages and democratic misuse. For the above mentioned reasons, the authors would like to resolve the specific role and the meaning of the manager of security and intelligence system with special needs who is managing in the field of functional and organizational adaptation of security and intelligence subjects to a new security environment. Also, they would try to put an accent on the importance of knowing organizational culture and its elements that are reflected trough the managerial knowledge of organizational values, organizational surrounding and managerial style. Modern security reality and all transnational challenges had conditioned a need for the exact analysis of corporative and other security partners, which had resulted in a general shift of security challenges. Due to that reason, managers should recognize the need to integrate security and intelligence services into institutional security frame of network units which comprise of state organizations, business, nongovernmental sector, citizens and international organizations. The consequence of excluding the above mentioned security subjects from the institutional security frame could be fragmentation, separation and independency of one subject in comparison to another which can result in negative consequence for citizens safety, national and global safety as well.*

Key words: Security Manager of, Security and Intelligence System, security, security challenges and threats.

INTRODUCTION

The definition of the intelligence service is a fundamental epistemological category and Pajević presents it as follows: "Modern intelligence service, as holder of an intelligent and specific institutional intelligence, strive by propagating, in accordance with the principles of intelligence, security and culture of the appropriate methodology, to predict, penetrate, and preempt threats to national security and to contribute to all who create and implement national security policy, in peace and war, in order to protect national security and conduct a national political agenda, with particular emphasis on the creation of conditions for optimizing resources and competitive advantage in relation to state, powers and the actors that pose a threat to national security" [7].

The role of managers in managing and directing the intelligence activities

Management in the intelligence-security system is a continuous process that initiates and directs intelligence (counterintelligence) and security activities for the efficient and effective achievement of objectives and tasks entrusted to protect national security. The result of the management process of intelligence-security system is the decision-making and its implementation in the intelligence activities. The result of the intelligence activities are certain final intelligence products (intelligence) and services (covert action) which satisfy needs of the state and political leadership (e.g., president, army commander, Prime Minister, etc), which is the basis for making wise decisions in the internal and external political plan. The term “consumers“ is often used for this category of recipients of the final intelligence products. The function of management is to allocate the resources to those activities of intelligence (intelligence and covert actions) for which there are observed and identified security needs and requirements in the socio-political process. It is deliberately emphasized *in the socio-political process* because intelligence activities are not related only to the area that includes the national territory, but on all the territories where there are the holders of threatening activities whose activities may directly or indirectly endanger the national security and national interests or the interests protected as a result of international institutional cooperation (e.g. NATO).

The ultimate goal of management in the intelligence-security system is meeting the consumer needs with the final intelligence products, where the subjects of intelligence and security systems appear as services in the political process and/or services such as covert actions. In this case, it appears as an instrument for the implementation of foreign policy decisions. Intelligence-security system is established to meet the needs of state and political leadership and society which has a permanent character. These elements represents the basis for the permanent management activities. To have a successful intelligence management, the management itself must understand the importance and significance of organizational culture and has knowledge of all its elements of which include: organizational values, organizational climate and managerial style.

The research of quality of information was motivated by problems of quality of information that have emerged in the organizations. A number of intelligence, military, economic and political initiatives have failed because of the problems in the information quality. The definition of information quality can be based on the perspective of a consumer of information and data perspective. The term quality is defined as the ability to use and this definition is widely accepted in the intelligence literature. Wang and Jaka define the information quality as the information quality that is appropriate for the consumers of information.

They argue that consumers are the ones who, at the end, decide whether the information products are suitable for use. However, consumers are not willing to find defects in the information, or change how they use the information. From the perspective of information, information quality can be defined as information that correspond to the specifications and requirements. The research on information quality is divided into two perspectives: management and databases. There is a combination of two perspectives: the high quality of information and without damage, possessing desired features [1].

The assessment of information quality (IQ assessment) is the essential for quality information management. The goal of quality information management is improving the validity and usefulness of information. Information quality management (IQ Management - IQM) is composed of three different areas of management: quality management, information management and knowledge management.

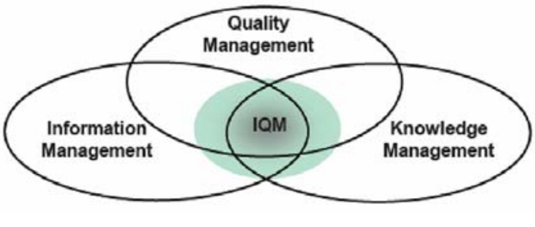

Figure 1. *Information quality management*

Management refers to the process of directing others to execute a certain task, while leading focuses on the ability to influence others who should execute some task [8]. Among many divisions and terms for each level of management, it seems logical to accept, based on systematic theory the following classification levels of management: immediate or operational level of management, middle or coordination level of management, strategic, supreme, principal, or the general level of management. However, despite significant research and organizational and practical interest, we have found that there are the positions which, under management style. imply some other phenomena with the same content. "Under the style of managerial behavior we mean optimal, specific, dynamic, stable and flexible synthesis of methods, tactics and techniques of management, which are immanent in the leadership and management system and which should be decisive for the inventive and creative execution of specific tasks" [4].

However, all previously developed management styles are mainly based on three basic types: "autocratic, democratic and style of individual freedom." Vršec has got a convenient and scientific approach – he accepts so-called general methods and styles. General methods can be a part of management system, whereas the name and the approach are consistent with the styles that we have defined. These are the "autocratic methods (consistent with autocratic style), the liberal method (compatible with the style of individual freedom), paternalistic methods (method of paternalism in the autocratic style), the democratic method (in accordance with democratic style), authoritarian-democratic methods (practical mix of styles)" [3].

In this sense, managing intelligence service is carryied out by performing various activities, which are often called (in the literature) "functions of a management process." In theory, there are different views on the number, importance and content of these activities. Management viewed as a process in this approach, can be analyzed from the standpoint of the holder of managerial functions, according to groups of activities performed by a manager of the intelligence services: "representing the organization to the environment, planning and programming work, and building and implementing systems of planning, organization of work processes, coordination and synchronization, control over the scope and quality of organizational units and individual employees, or recording or developing and application of information systems of organization, analysis of implementation, evaluation of results, communication (intraorganizational and toward the environment), solving the current problems and conflicts, etc. [3] In this context, managerial staff has the following tasks: design of intelligence research, coordination and subordination of all organizational units, data protection, development of intelligence methodology, respect for human rights and freedoms, energetic and proactive approach, etc.

Managers of the intelligence organization represent a primary organizational, actional, and mobile element needed for realization of the state function of the intelligence and its objectives. Managers should be familiar with security issues that are part of their activities; they should also have an impact on the creation of professional policies and defining of program tasks of the intelligence [9].

The attitude of the intelligence towards the future is very important in the philosophy of manager's plans. The degree of ambition varies from manager to manager, as well as from intelligence to intelligence. A number of intelligence and security services is preoccupied with the present and solves urgent and not important security challenges, threats and risks. Many intelligence and security services are preoccupied with correcting errors made in the past. A proactive attitude of management is reflected in the acceptance of change as something that is normal and the willingness to initiate structural changes, not just an incremental character. Inspired by the concepts of Russell L. Ackoff, an American scholar in the field of organizational theory, many experts studied the approaches of a manager as a subject of intelligence-security systems towards the future. In this regard, we have considered four positions: nonactive, re-active, preactive, and interactive. Although not having been made on the basis of a broad empirical analysis of intelligence planning practice in many countries, this systematization constitutes quite a good approximation to the actual situation in the intelligence practice.

Non-active or vegetative approach means that managers of a subject in the intelligence-security system reconcile with current developments and plans on the basis of features, avoiding any sensitive risk. They do not look for the optimal solution, but they are satisfied with so-called *the second best solution* (satisfying results or results "Day after day", i.e., to meet daily needs). The objectives are adapted to the possibilities of the the subject of intelligence- security system. In practice, managers of intelligence and security agencies often complain about not having adopted the proposed budget decision to the legislative and executive branches of government; allegedly, restrictive measures can be the reason for the lack of possiblity to plan and implement prevention programs. Of course, a proactive approach requires adequate budget, but this is not the only variable that would discourage managers to take active preventive orientation.

Reactive or repressive approach means that managers of subjects in the intelligence-security system try to avoid problems and resolve problems as they did it in the past. There is nostalgia for past times. Unlike non-activists who "swim with the stream", reactivists "swim against the tide". Reactivists are susceptible to recurrences of the past, and often such managers may hear statements that relate to the period of the previous "golden age in which you could sleep in the park and cover yourself with the newspaper, and being sure no one will compromise your safety". Often, this type of a manager grieve for reprisals (repressive measures such as police powers: arrest, detention, use of force, informative talks, wiretap telephone and other communications, etc., which should have the intelligence service).

Preactive or proactive approach means that managers of subjects in the intelligence-security system accept orientation toward the future and have a positive view to the changes in the environment in which they carry out the intelligence activities. Managers favored analyzing the changes that may have adverse consequences on national security and interests. Management is focused on predicting the future course of events in society and strive to create strategies to adapt to anticipated security challenges and threats carried by the new global changes. Managers of the intelligence are seen as the planners, not as prophets. The similarity of the planners and the prophets is that both sides are able to predict the future, and the difference is that the planner can control the future, and it affects the perceived trend of its achievements. Hence, planning is not fortune telling, but the process of controlling the future.

Interactive or futuristic approach means that managers of the intelligence and security services are oriented to the future. The assumption is that the future can hardly be absolutely controlled, but can be changed. Managers of the intelligence and security services are trying to create opportunities for growth and development of positive security trends in society, that induce economic, social and political processes. They strive to solve problems, not only on the basis of past experience (feedback), but with a view forward (feedforward). They consider technology as a significant factor in the development, but at the same time as something that can have both good and bad sides.

All intelligence agencies must deal with standard administrative matters, but the nature of intelligence operations makes many of these functions more complicated than those in the industry (private) or other parts of the government. "These functions include human resource management, security, training, communication, money management and logistics. The last three functions are very sensitive in the intelligence community, for several reasons, and would not be surprising if intelligence service pay more attention to them" [9]. One of the biggest obstacles to create an effective intelligence community is a bureaucratic internal organization, especially when it comes to several intelligence organizations.

Contemporary management of Security-Intelligence Network

Contemporary security and all transnational challenges have caused the need for the exact and eventful analysis of corporate and other security actors, which led to a general shift in terms of confronting contemporary security challenges. Accordingly, Fry and Hochstein emphasize that the intelligence service should be integrated into the institutional-security framework - *network of units*, which include, in addition to state agencies and security services and institutions, non-governmental sector and international organizations. Not including one of the security subjects in the institutional framework of security results in fragmentation, dispersal and independence of some subjects from others [2].

In this context, Johnston and Shearing advocate the application of the *node* based on networks, rather than the central concept of the state government. The authors offered "four sets of governmental nodes: a state set, corporate set, a set of non-governmental state organizations, and informal or set of volunteers" [2]. McGrew believes that the process of globalization caused that the police and the security-intelligence field of activity manifests itself in three dimensions: the level of *deepening* to increase interaction between local and transnational development, *expansion* of the sector with entities involved in management, and spatial *stretching*, so that a security event in one part of the world can have an immediate impact on global security plan. The three main sectors identified in figure No. 2 coincide with the already mentioned organizational model "state (bureaucratically-hierarchically organized), the corporate sector (competitive in the market) and non-governmental organizations and associations of volunteers. There are, of course, many divisions within each of these sectors" [2].

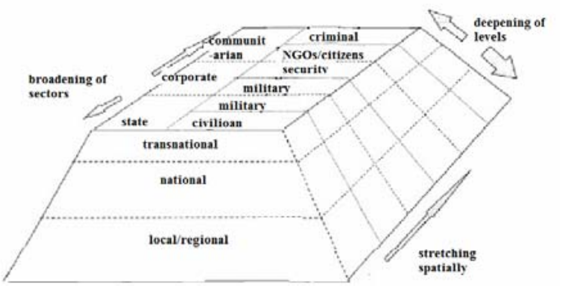

Figure 2. *Security-Intelligence Networks*

Networks can be developed within and/or between any of these three dimensions. Country or corporations will often appear as "the dominant node or partner in the security networks. Johnston suggests that, in general, the most productive thinking is directed to change the form of creating and managing institutional-security framework in which the individual fragmented parts of the state will interact with commercial, civil and volonteer subjects in domestic and global level. In this regard, Deibert points out that "transnational network of citizens-activists should be incorporated in the interactive state structure. Security companies and non-governmental organizations that have the intelligence capacity should be networked in order to create the function of protection of security. It would be useful. Security companies and NGOs through the networking form work within a number of specific states and localities. It is a form of multilayered governance. The development of local security networks between agencies, public, private and civic groups, provide clear examples of cross-sectoral networks, and other examples can be found at the regional, national and transnational level" [2].

It is clear that there must be some common interest to meet the actors in the network. It is not difficult to establish an interest shared by many Western countries, and corporate security providers. It can be summarized by the principle of neo-liberal tendencies to the market that provides services. However, the actual nature of the relationship must be subject of the empirical validation, and conflicts can arise between "nodes within the network" (author's note: entities in the security system). So, within the public sector the agencies may have different mandates and objectives that are sometimes overlapping, sometimes not. Corporations could not agree with some joint projects taking into account that they can be in a competitive relationship. Opposition will be resolved, depending on the relative power of actors. In some cases, they can lead to a restructuring of the network. Therefore, one must not forget the impact of security networks and the tasks that are in focus. "One should bear in mind that particular groups which have security as the primary objective may, under certain conditions, become part of the network. Similarly, the way the targets react, trying to collect information and perform some repressive act, can have an impact not only on specific operations, but also on the form of a network" [2].

Management is essentially a matter within the state hierarchy and essentially represents the application of appropriate rules and procedures according to the level of responsibility. Discretion is a very important feature of the intelligence and other security services activity, while the network is characterized by fluidity, which is also their strength. In this regard, Kickert and Koppenjaan indicate that the network management has got two important functions: *game management* and *network structuring*. "Game management includes the following measures: (1) activism involves activation of the network in order to solve individual problems and the involvement of those actors who can help (2) mediation gathers an entirely different range of actors, problems and solutions, and (3) simplification involves the creation of favorable conditions for development." Network structuring takes transnational place in the world (for example, when the Berne group was formed it was comprised of six European internal security agencies, and now includes seventeen) [2, 13, 14].

CONCLUSION

The intelligence-security system is viewed as a complex economic, technological, sociological and organizational subsystem of the political system. The focus is on the ability to perceive the long-term consequences of current decisions. The dominant orientation of some of the intelligence and security services in the management is the following: in the past - reactive, in present - inactive, in the future – preactive, and also intelligence and security services are interactive. This means that they observe past, present and future as distinct, but inseparable aspects of planning, being very similar in focus. The interactivist orientation is based on the assumption that all three elements of time should be taken into account in planning.

The intelligence and security services are not only interested in achieving the objectives of existing national security, but also in formulating new objectives which should contribute to efficient and effective prevention, confronting contemporary security challenges, threats and risks; both at the national and at the international level. They are all equally in the focus. The interactivist organization is based on the presumtion that the three elements should be taken in account in the process of planning. The fundamental purpose of interactivist planning is changing the present state of intelligence and security services to fit the sketch of a desirable future. It is not desirable that the intelligence service on the basis of this orientation creates a conception of the future based on projections of the current situation. The intelligence and security services can not control all the elements and factors that may have negative consequences on the security reality.

Non-activist and reactivist approach of managers is archaic and inconsistent with modern organizational and functional adaptation of intelligence security challenges. This approach does not only have limited contributions to the security area, but also questions the existence of such organizations in the security system. Preactivists insist on adapting whereas interactivists insist on the impact on the future. Such a division is possible and it certainly has a place on a scienctific and practical level. These approaches are not incompatible, they can be combined. Undoubtedly, the interactivist approach is more progressive than others, but the truth is that all entities in the intelligence-security system are not always capable to apply it. Managers of proactivist and interactivist type have an intention to define variables (security challenges, threats), then create assess of the ability and restrictions, as well as security trends of the major factors that are essential for the results of intelligence. Both approaches require to observe and analyze the efficient and effective courses of action and monitor their effect on the social-security interests.

Countering threats to the dominant and non-state actors not only requires the engagement of intelligence. In fact, opposition to contemporary security challenges requires a transformation of the security sector. Dominant threats can be confronted only if all the actors, which are authorized to deal with contemporary security threats, are in the required communicative network. Therefore, the existing guidelines, processes and structures should be transformed. The goal of transformation implies the strengthening of management and the establishment of effective processes and structures commensurate with the challenges to confront. Three principles form the core of the transformation programme are: management of central security networks, cooperation and the orientation of intelligence capacity.

Management of central security network refers to the systematic connection of the four areas. The first area includes all of the security sector entities which are authorized to confront contemporary security challenges. Second – it is based on all levels of decision making (internationally, nationally and locally). The third includes all security instruments. The last area refers to all tasks that are to be realized. Management of central security network puts the emphasis on cooperation between the security sector entities, and between this sector and the relevant third party. An integrated approach to security, however, expands the understanding of cooperation outside traditional boundaries in two ways. First, the operations are proportional to new security requirements which requires coordinated interaction between all stakeholders. The joint action of all actors in the security sector is needed to increase the efficiency and effectiveness. In addition, a common approach is a prerequisite for the second sequel of cooperation: cooperation with third parties and the business sector. Both the sequels of cooperation must take place at the national and international levels, because no national agency alone can deal with contemporary security challenges.

The above mentioned insights and reflections can serve as a basis for making relevant conclusions and recommendations (de lege ferenda) for the application of the presented model of management and functioning of the intelligence process and professional standards. They can serve as a model for functional and effective intelligence operation, not only for the intelligence, military and police, but also for other institutions which rely on intelligence in their work.

REFERENCES

[1] M.Ge, M.Helfert: „A review of information quality research“, develop a research agenda, in ‘Proceedings of the 12th International Conference on Information Quality’, 2007, http://mitiq.mit.edu/iciq/pdf/a\review\of\information\quality\research.pdf (7.1.2012)

[2] P.Gill, M.Phythian: „Intelligence in an Insecure World“, United Kingdom: Polity Press, 2006.

[3] M.Jurina: „Rukovođenje i organizaciono ponašanje“, Zagreb: MUP RH, 1994.

[4] R.Masleša: „Organizacija i funkcionisanje policije u demokratskom društvu“, Sarajevo: Fakultet kriminalističkih nauka, 1999.

[5] M. Pajević: „Obavještajni kapital“, Human, Vol. 1, 2011, No. 1, 9 - 18.

[6] M.Pajević: „Preventivna uloga obavještajne službe na nadnacionalnoj razini“, Godišnjik na trudovi (Zbornik radova), Evropski Univerzitet Skoplje, 3(3), 2011, 499. - 518.

[7] M.Pajević: „Uloga obavještajne službe na zaštiti nacionalne sigurnosti“, Međunarodna naučna konferencija, Zbornik radova, Evropski Univerzitet Skoplje, 2012, 207. - 224.

[8] P.Sikavica, F.Bahtijarević-Šiber: „Menadžment“ Zagreb: Masmedia, 2004.

[9] D.Vejnović: „Državna bezbjednost - obavještajne službe“, Banja Luka: Glas Srpski, 1995.

BIOGRAPHY

Maid Pajević was born in Mostar in 1977. He obtained his PhD from the Faculty of Criminalistics, Criminology and Security Studies in Sarajevo in 2010. His thesis was entitled "The Role of the Intelligence in the Prevention of Modern Security Challenges." From 2000 to 2010 Pajević was employed at the operational and managerial positions in the intelligence-security system in Bosnia and Herzegovina. Since 2010, he has been working as a lecturer of Criminology at the Agency for Education and Training of Police Personnel of Bosnia and Herzegovina. He is also working at College "Logos Center" Mostar as a Head of the programme "Security Studies".

JAČANJE MENADŽMENTA U OBAVJEŠTAJNO-SIGURNOSNOJ KOMUNIKACIONOJ MREŽI

Maid Pajević, Armin Kržalić

Rezime: *Sigurnosne i obaveštajne službe su danas sve više izložene javnoj kritici zbog izvršenih terorističkih akcija koje su imale za posledicu stradanje velikog broja ljudi i nanošenje znatne materijalne štete. Efikasnost i efektivnost sigurnosnih i obaveštajnih službi se posmatra kroz percepciju sledećih pojava: operativni neuspesi, organizacioni nedostaci i demokratska zloupotreba. U vezi s tim, autori u članku žele rasvetliti specifičnosti uloge i značaja menadžera sigurnosno-obaveštajnog sistema sa posebnim osvrtom na, sa jedne strane, upravljanje i rukovođenje na polju funkcionalnog i organizacionog prilagođavanja sigurnosno-obaveštajnih subjekata novom sigurnosnom okruženju i, sa druge strane, akcentovati važnost i značaj poznavanja organizacione kulture i svih njenih elemenata koji se reflektuju kroz menadžersko poznavanje organizacionih vrednosti, organizacione klime i menadžerskog stila. Savremena sigurnosna zbilja i svi transnacionalni izazovi su uslovili potrebu egzaktne i sadržajne analize korporativnih i drugih sigurnosnih aktera, što je dovelo do opšteg pomaka na planu suprotstavljanja savremenim sigurnosnim izazovima. Shodno tome, menadžeri trebaju prepoznati potrebu da se sigurnosne i obaveštajne službe integrišu u institucionalno-sigurnosni okvir mrežnih jedinica, u koje se ubrajaju, pored državnih organa, i poslovni, nevladin sektor, građani i međunarodne organizacije. Neuključivanje naznačenih sigurnosnih subjekata u institucionalni sigurnosni okvir ima za posledicu fragmentiranost, raspršenost i nezavisnost jednih subjekata od drugih, što može imati negativne konsekvence za sigurnost građana, nacionalnu i globalnu sigurnost u celini.*

Ključne reči: menadžer sigurnosti, sigurnosno-obaveštajni sistem, sigurnosni izazovi i pretnje.