Challenges of Democracy and Asymmetrical Threats – Military Organizations By Means of Learning and Adaptation toward the New Capabilities and Knowledge

Dario MATIKA, Robert FABAC,
Institute for Research and Development of Defense Systems,
Ministry of Defense, Croatia

Abstract. Contemporary civil-military relations are marked by new social phenomena, by democratic movement evolution as well as by new emerging forms of threats and aggression. The traditional vision and mission of armed forces has to be changed. Transformation requires a complex process of learning and organizational changes that should create new capabilities and competencies. Army should develop its capabilities within new core areas such as *Crises Management, Law Enforcement, Detection and Response*. Besides that, military activities must be transparent and determined by issued strategic documents on national and higher levels. Military high-tech proliferation, networking, strong growth of information usage and communication technologies supported by traditional human ambitions in conquering power and resources result nowadays in the emergence of new, asymmetrical threats. Terrorism is one of such threats. While in the past, informal groups uncontrolled by authorities were less dangerous because of their threat assets' low-level damages, nowadays the situation has changed. New asymmetrical threats are potentially globally dangerous and they pose very new challenges to regular military forces, which should prepare themselves in a new manner and learn new organisational responses. One kind of effective military reaction is forming alliances, namely by better connecting and networking of military forces. Democratic and civil society achievements, as well as new threats, make the modern army's mission more complex. Capabilities and competencies of non-intrusive behaviour are required; the commitment towards *non-invasive* methods is desirable as well as the preservation of human lives. Paradigms of military non-intrusive and indirect behaviour likewise create an imperative for adapting the military organization that needs to improve itself by both internal task owners' activities and by external, civil environment factors.

Introduction

Contemporary civil-military relations as well as national security systems are influenced by new social phenomena – evolution of democratic achievements and by new forms of threats and aggression. The traditionally accepted vision and mission of military forces should be changed and transformations require a complex learning and organizational process of change, while new capabilities and competencies must be created.

On one hand, civilization achievements of modern states require that the basic rights of domestic and foreign citizens are respected. Freedom of travelling and trading can be recognized among these rights and for that very reason the response to asymmetrical threats requires interference in these rights of the citizens. New threats, especially terrorist threats, require a response that cannot be achieved just from the military sphere, nor from the sole usage of military power. For addressing those issues a complex context is needed which incorporates economy, politics, ideology and religion. Therefore, an important defence and security component is the civil part of system and the orientation on security through non-destructive and non-invasive methods.

Therefore, the security and defence system (SaDS) is perceived from the prospective of managing complex organizations that go beyond constraints of fragmented approaches. Borders of certain areas («trans-areas») and both characteristics and requirements of the contemporary environment (uncertainty, complexity, ambiguity) are addressed by the new capabilities' development and use.

1. Modern Security and Defence Systems

1.1 Requirements toward Organizational Security Systems

With respect to threats and conflict – **peace, crises (low-intensity conflicts), war –** the contemporary SaDS must meet criteria in order to function successfully in those three states. Because of a complex organizational structure, the national SaDS should use in its activities recent solutions from three organizational management paradigms – **organization of the government sector (public administration), military organization and corporative sector –** with respect to responsibilities and the approach towards planning activities both civilian and military. It is important to observe that in each dimension different options are not excluded mutually. Their appropriate adjustments are essential.

These three requirement sets or the so-called «requirements cube» (Illustration 1.), create new *operative tasks* for a vast number of present SaDS undertaking their internal reforms. One important spectrum of obligations refers to new military capabilities (peace, crises «cube»). Asymmetrical threats, terrorism, human trafficking and materiel smuggling represent a big challenge for security of the contemporary world. Therefore, new functional national security and defence capabilities are necessary for a satisfactory response to new challenges, and these capabilities are related to the areas of Crisis *Management, Law Enforcement, Detection and Response.* Certainly, the bigger part of organizational structure with that knowledge belongs to the *non-military security sector*.

In order to manage successfully SaDS in a relevant strategic situation the SWOT analysis (internal strengths, internal weakness, external opportunities and external threats) is often applied. In case of security and defence the system analysis is to a certain extend reduced to the area of orientation towards the outside *threat*. At the same time, the state of the internal system should be mainly analyzed for weaknesses. So, let us demonstrate this model as S**W**O**T**. The state of external analysis and internal weakness (formula 1) should be given in the strategic analysis regarding security issues:

SWOT ⟶ S**W**O**T** (1)

The period of peace is marked by potential threat, military capabilities need not be at the maximum and principles of efficient budget use are important. Rules of strategic management and models valid in state administration and corporations were put here in focus. During crisis periods, key capabilities, especially new ones, should be developed and fast reaction and strength of potential operative actions should be optimized. The level of military potential should be variable with the corresponding dynamic of change. Regarding this, care must be taken of the modernization moment for defence systems, as well as of new technologies' development and diffusion. In crisis or war scenarios, paradigms for strategic management of military organization dominate.

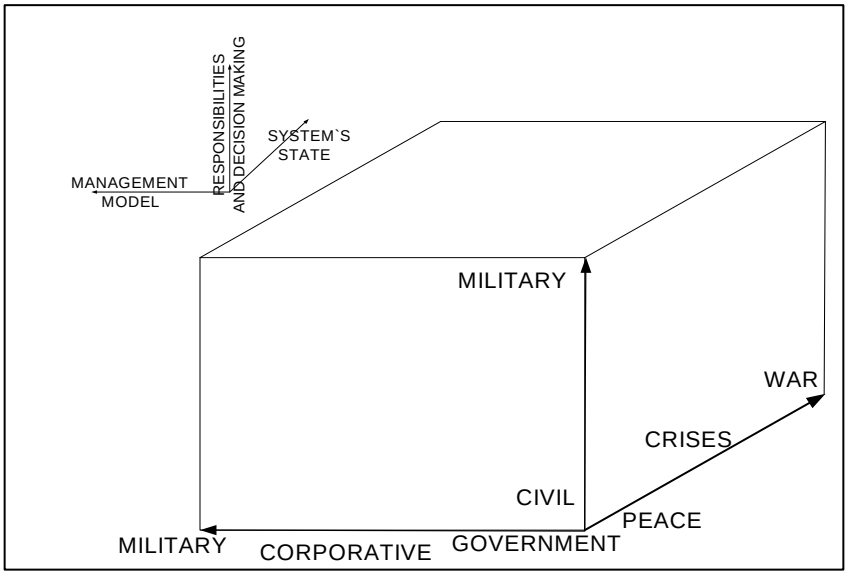

Illustration 1. «Cube of requests» toward security and defence system.

Besides the military component, the broader concept of national and multinational security encompasses also economic, political, social, ecological components. Security exists in a situation where danger is not present enabling under such circumstances the possibility of free development of individuals, groups and nations.

1.2 Security Challenges and New Response Capabilities

During the cold war period, the two sides were running a competitive race and by building their own SaDS, they strengthened their military powers inside paradigms of preparing classical (even nuclear) combat. Dominant doctrines were deterrence, localized conflicts and non-use of military power. The current world order is marked by great dispersion of political, economical and military power over numerous international actors. One popular definition of social conflict depicted it as confrontation of individuals and groups, on basis of competitive interest, different identities and/or unequal attitudes. In cases where numerous players participate of on the strategic scene, the context of potential conflict becomes more complex and new circumstances with diverse forms of threats and aggression should not be a surprise.

New and conceptually different security challenges emerging after the breakdown of the bipolar military relation model do not have all classical military attributes. We are talking here about questions related to ethnics, national and religion issues, undefined borders, uncontrolled

migrations, refugees, environment pollution, organized crime, WMD and dangerous material proliferation, terrorism.[1] It could be said that the present negative elements of the security environment in Europe are concentrated in threats caused by the phenomena of specific situations of certain states' development (Bosnia and Herzegovina, Serbia, Albania), geographical proximity to higher risk areas (North Africa, Middle East) as well as ambition towards a new division of interest spheres.

The «request cube» in new circumstances of asymmetrical threats and conflict domination must give satisfying responses also regarding the model of civil-military approach toward the planning process and the model of strategic management, inside which methodology is improved continuously and new cognitions are adjusted (referring to threats and opportunities).

Through optimized budget spending, a certain SaDS operational quality level is needed in peacetime. In the sphere of rational resource management, various support models are used (PPBS, Balanced Scorecard). Recent approaches to strategic management in the corporative sector [2] with the tendency of increasing influence in the security sector are aimed toward development and functional capability upgrades, *knowledge management,* core competencies concept, learning organizations, maturity in organizational processes.

A pre-requirement for developing organizational capabilities is advanced organizational learning. According to one accepted definition »…learning is a process by which knowledge is created through experience transformation and can be described as enhancement of capabilities for taking an effective action…» (Kim, 1993, p. 38).[3] SaDS perceives efficiency as finding good responses to new challenges (crises, terrorism) which can be obtained through capabilities (developed through purposeful learning). Organizational learning and knowledge management imply certain processes running, where knowledge is transformed in ways of socialization, externalization, combination, internalization.[4]

While in the past stockpiling of weapons dominated, recently this process has transformed itself into a competition of permanent improvement of organizational capabilities and core competencies.[5] New relevant capabilities are within the area of resolving CBRN threats, detecting (identifying), preventing, neutralizing and non-invasive methods.

2. Responses to New Threats

New security threats, the so-called asymmetrical, emerged in the 1990's and have been dominating this century. They are special and deserve attention because of several phenomena among which we emphasise:

a) Highly developed means of destruction and their availability. Globalization, besides technology diffusion, especially of dual-types, has enabled individuals and small groups to become potentially very powerful and some authors call that appearance «privatization of war».[6] Groups that do not obey to formal national and international authorities and which represent non-state actors could potentially cause great damage to society and its development.

b) Highly developed national infrastructure, such as energy system, communication, transport, which has been generated for years along with a long-term history of growing and facilitates the state and economy to operate at a respectable level. Water and food production and distribution are a part of vital infrastructure that should be protected. Possible attacks on objects and flows (energy, communication) of crucial importance for

society functions produce, besides negative effects due to human victims and material damages, also huge negative collateral impacts – economy degradation, fear and uncertainty and slow down development processes.

New threats are potentially globally dangerous and they set new missions for national and international defence systems that should prepare them in a new manner and to "learn" new organizational answers (responses). Searching for solutions through exclusively traditional military approach and repression is not satisfactory. Citizens and infrastructure security require *capabilities* primarily from the areas of recognizing, preventing and preparing non-destructive responses. Integral security systems require improvements of internal trans-organizational processes and technologies (equipment, tools).

2.1 Components of the Security and Defence System – Knowledge Management

The European Security Strategy (2003) emphasis *Coping with Threat,* as one of three strategic goals: "Response is not possible just with military means. Coordinated activities of diverse actors and synchronous uses of economic, political, diplomatic and other mechanisms are necessary." The Action Plan for Combating Terrorism approved at the meeting of the Political and Security Committee stresses among main goals – international participation, greater efficiency of the EU working bodies, traffic and border security and prevention of access to financial sources. Evidently, the military component does not have the main obligations and the civil sector is also included. After the *September 11* attack, US civilians realized that strategic studies still represent a discipline worth their intellectual efforts.[7] This fact illustrates the comprehensiveness of the «cube of requests» and its dimensions.

The National Security System can be analyzed according to its functional (activities, operations) and structural segments. When talking about the structures, it should be noticed that it contains external and internal security elements.[8] Besides the armed forces, the internal security includes the civil defence segment. Such approach is characteristic for Croatia, as well as for other countries emerging in the area of former Yugoslavia. Civil defence is organized as civil protection, war preparation of the economy sector, observation and report and information and communication. Interesting is that activities and war and crises preparations of non-armed forces in certain SaDSs existed even before the period of shock of terrorism.

Besides establishing a network of connected civil-military units from SaDS able to confront the terrorism network, human aspects of organizational structure must be well supported by the high-tech component. In the book «War and Antiwar»,[9] the concept of knowledge in the security context takes a special place. Military personnel and civilians, the so-called «knowledge warriors» are highly devoted to paradigms of the third wave of economy (agrarian, industrial, informational) and this is manifested characteristically in the approach to military and war – society of information, rapid technological changes and civilization heterogeneity. How important technological innovations are, is well illustrated by the fact that the 2005 US defence budget was 402$ billions and approx. 17% (69$ billions) were assigned to research and development.

Modern corporative strategic management (Illustration 1.) in security and defence system focuses on the concepts of *knowledge management* as a commitment for obtaining critical responses to *organizational adaptation, survival and competitiveness* in situations of discontinued and surprising environmental changes. New asymmetrical threats represent exactly that sort of outside challenges and changes. Organizations must learn, and sometimes adaptation

is not enough, that «second loop» learning, generic learning,[10] is essential for reaching new performance capabilities.

During the *Cold War,* opponents were compared and competitive behaviour of great powers was significant. Theoreticians often described that through the «zero-sum game» model. In new scenarios, competitiveness should be perceived as an occurrence between national security systems and non-state groups (criminals, terrorists) that do not accept international and civilization laws and norms. Competitiveness takes place in new circumstances. What matters in each framework is the *speed of organizational adaptation* (fast learning) enabling the achievement of certain competitiveness levels (by functional capabilities).[11]

2.2 Conflict Scenarios and Risk Management

The unexpected challenges scenario in the context of two opponents' conflict can be described well by the Boyd Cycle's formal framework (Illustration 2.). [1] The cycle starts with perception followed by orientation, an internal process that gives sense to circumstances. In simple tactical situations, one should pass as fast as possible through the cycle which enables success. In case that during the opponents-orientation phase, it is possible to make an impact on his mental paradigm or attitudes and his «believes» are not suitable enough (surprise of terrorism), then the impossibility to overcome external challenges and make good decisions creates the feelings of uncertainty, confusion and fear. This model should be applied when it comes to preparing a response to asymmetrical threats and aggression.

In situations of unexpected challenges, uncertainty and potential risk the *concept of risk management* is important. Each risk management methodology starts with activities of perception and so does NATO in its documents referring to its own adaptation and certain strategic elements for its further development usually have *perceptions of security threats* as their first topic.

The security concept refers to people and infrastructure. Referring to the security of industrial objects and companies of special importance, the methodology of *risk assessment and management* (RAaM) involves in its approach: recognition of critical infrastructure and assets, assessment of importance, threat assessment, vulnerability assessment, risk calculation and essential measure identification. The risk magnitude depends on factors of threat, vulnerability and vitality. Measures common in risk treatment include selectively reinforced uses of high-tech and similar equipment for protection and similar purpose.

Today, state agencies should have the capabilities and practice of using RAaM methodology pursuit that certainly belongs to the *new capabilities* relevant for national security. Crucial infrastructure should be recognized and protected by legislation. This assumes military and civil activities and processes for an efficient response to asymmetrical threats. Different risk management methods from strategic to lower levels are present in defence systems in most of the developed countries.

[1] Boyd circle concept or OODA (observation-orientation-decision-action) was created in the 1970's. This idea originates from Colonel John Boyde who analysed the air-to-air battle with his model.

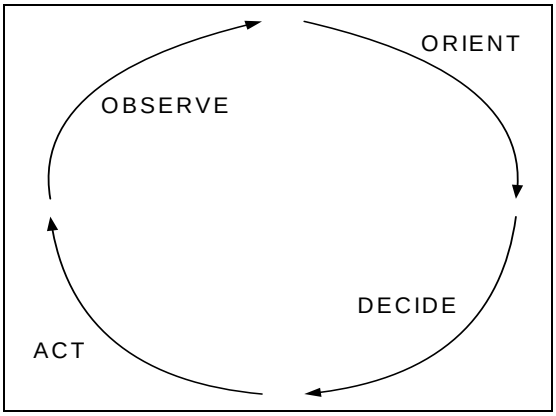

Illustration 2. Boyd Cycle.

The US strategy (often called Bush strategy) has a determinant according to which it is necessary to make a *pre-emptive strike* due to a wide spectrum of WMD, possibilities for its production and distribution and the impossibility of peaceful blocking of these growing threats. It could be said here that this is risk-management in a "less sophisticated" version.

2.3 Organizational Changes – Alliances and Networks

In the sphere of systematic elimination of weakness and due to occurrence of intensive challenges, organizational learning has become an imperative not only in form of adaptation, but also in form of the generic type, especially with learning leaders and managers who are decision-makers.[2] At the organizational level, knowledge implementation should result in effects related to successful balance through the «demand cube»:

- development of new capabilities where weaknesses are recognized through S**W**O**T**-analysis would be eliminated,
- organizational structure transformation, building of effective alliances (international) and also of networks and virtual organizations (civil-military), key process reengineering;
- commitment that new SaDS organization should expand responsibilities in areas different than just the *armed forces*,
- larger investments in research and development and in appropriate education and training.

In the military-political sense and in the economic milieu, alliances are very important, especially in the context of preserving national and international security. Strengthening European security is based on better affiliation among European countries. NATO alliances represent the greatest concentration of military power in the world. Numerous theoretical definitions regarding alliances include motives for forming alliances – strengthening of negotiating position, reducing existing threat, increasing of military power. The key mechanism lying in the background of forming alliances and networks might be the optimal use of resources and capabilities and their transfer between strategic partners.[12] The realization of military and political-military alliances moves towards development and exploitation of superior resources following the philosophy of resourced based view (RBV) in corporative strategy.

[2] Generic learning or double-loop learning implies the change of mental concepts (maps) of decision-makers.

If we consider a strategic situation in which the security system chooses to associate with some complementary organization from the environment, then we are talking about recognizing opportunities (SW**O**T) for achieving greater internal strengths and eliminating weaknesses. Networks and virtual organizations represent potentially effective, multidimensional and multifunctional forms that can provide responses to challenges of asymmetrical aggression.[3] The potential utilization of other organizational forms in Europe, except the armed forces, is support by the French initiative (Political and Security Committee, July 2004) for establishing European Gendarmerie Force. The concept of police forces with military status is a characteristic of several European countries, but the establishment of gendarmerie forces disposed to the EU as well as to NATO and UN is significant. Dual control (civil and military) and qualification for low-intensity conflicts are the advantages of organizing gendarmeries force.

In line with the integration with non-military institutions, the transformation of great organizational systems such as NATO takes place. Expectations regarding the collaboration between NATO and American policy[13] are the most intensive in the area of peace and humanitarian operations, WMD proliferation, activities during crises and disasters, i.e., far from being only restricted to military elements.

A new SaDS organization means cooperation between military, police, local civil defence, government crises agencies and private sector. Reactions to crises should be trained and for that purpose simulation tools are useful. The main processes in network security organizations are important for these systems due to trans-organizational characteristics. Therefore, it is vital that they are well designed and several approaches are valuable, such as *maturity models*.

2.4 New Capabilities in Security Systems – Non-invasive Methods

New circumstances regarding security problems require also suitable laws and regulations, but today regulatory rules range from authorizing governmental institutions to pressures of democratic tradition referring to greater individual freedom. States aspiring greater social capital take care of human rights and freedom. According to Diamond, highly civilized societies should be characterized by culture of trust, cooperation, reciprocity, respect, tolerance and compromises.[14]

Therefore, today the armed forces' role and importance in society incline towards protection role. Operating should be transparent and determined by accessible strategic documents. Capabilities and competencies with non-invasive attributes are desirable as well as commitment towards both the preservation of regular functioning of civil society components and the unrestrained development of individuals. According to the new roles, security systems and military organizations should reform, adapt and improve themselves.

Conceptually considering strategic situation for a general national security system nowadays, we use SWOT analysis. Besides the statement regarding the expression (1), we would like to stress at least two facts that are important but not always noticed in the real world.

The first fact is the characteristic of threat level (T) for which we claim that it has a relativity character depending on the focused state. The risk assessments for Croatia made in the

[3] While the block competitiveness is well described by models of non-cooperative game theory models, for alliance models cooperative models are useful (with coalition concepts etc.). See e.g.. Owen, Guillermo: Game Theory, Third Edition, Academic Press Inc., 1995.

analysis of the publication Croatia Defence & Security Report Q1 2006 [15] are given by the results:

(Inter-state, Terrorism, Crime) = (62.9; 74.0; 57.1)

(2)

Composite Security Risk = CSR = 64.7

According to this assessment, Croatia is in the 12th place in her region according to total CSR indicator. In terrorism risk assessment, we are in the 11th place. However, we believe that the same level of terrorist threat for Croatia does not necessarily mean the same damage (vulnerability) for other countries in this region (Illustration 3.). Croatia, a country with Mediterranean atmosphere and culture, is a country of tourism and pleasure for ordinary people. Therefore, our *area of weakness* is expanded within the framework of new asymmetrical threats. A potential attack could significantly lower our economic potentials by damages in e.g. tourism sector. Connections between sectors, privatization of tourism capacities, which are now predominately owned by foreign companies, lead to the phenomena of possible collateral damages.

As above-mentioned, the risk magnitude depends on threat, vulnerability and vitality factors. Therefore, regarding the internal characteristics of certain states the same security threats do not generate equivalent potential negative effects. Illustratively, the framework that applies in the S**W**O**T** analysis and determines strategic position depending on a particular country moves in the space for two arbitrary countries A and B (Illustration 3.). As we stated earlier, it is appropriate to look at W and T dimensions for security analysis. A universal measure for threat does not exist or it could be said that equal threat due to characteristic internal strengths and weakness results in unequal «negative area» threat –weakness (Illustration 3.).

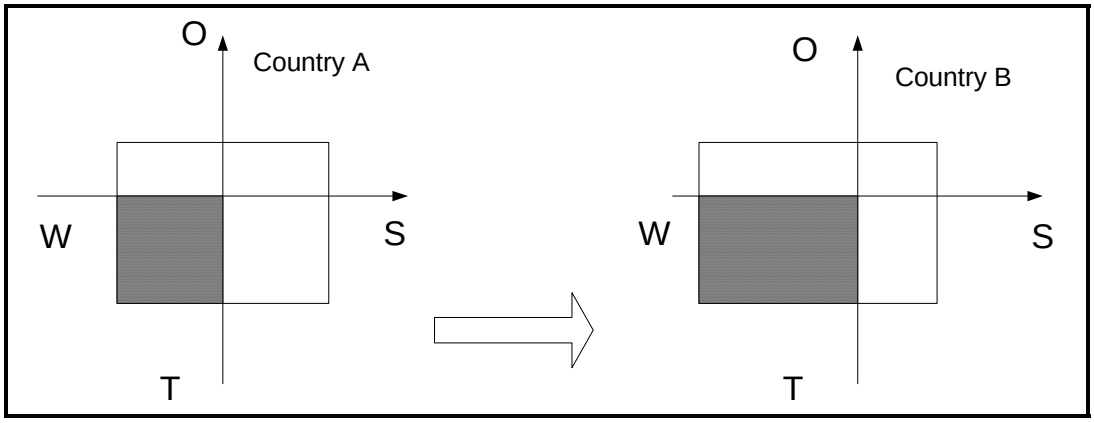

Illustration 3. SWOT analysis for different countries

Surely, the linear approach in defining «composite security risk» must be modified. Images of attractive tourist destination make Croatia particularly sensitive (W) to asymmetrical threats. Weight factors belonging to variables (x_1* Inter-state, x_2* Terrorism, x_3 * Crime) in CSR generally need different values:

$(x_i,...,x_n)$ and $x_i \neq x_k \; \forall \; i,k$ and $\Sigma \, x_j = 1$ (3),

whereas x_i are variables whose values depend on particular country.

Besides the *weakness* (W) area for Croatia, the above-mentioned publication points out in the security SWOT analysis the following in the sense of the traditional security concept:

- ✓ history of tensions with neighbours,
- ✓ long experience with drug and human trafficking, material transit;
- ✓ relatively long borders

Apart from characteristics related to «relativity of threat», the particularity of increasing internal strengths as well as eliminating weaknesses should be also stressed. Reduction of **W-T** area (Illustration 3.) can be achieved by decreasing or eliminating threat or by improvements of the internal weaknesses situation. While decreasing asymmetrical threat is sometimes outside the area of narrower security context (foreign policy etc.), management of weakness dimension (W) seems to be a relevant option. Removing certain internal weaknesses in the past was often achieved by increasing repression (control of citizens, police tracing, holding in custody) that is not acceptable anymore for most countries including Croatia.

If the intention is to reduce weaknesses (W), then the **response** to this requirement lies primarily in the sphere of new capabilities, especially in non-invasive methods and non-destructive reactions. Activities recently becoming more important are detection, recognizing, prevention, protection and neutralization. High-tech equipment is accompanied by sensors, detectors and DNA technology. In this sense, organizational *intelligence* departments play also an important role.

This response model is familiar with other so-called «soft elements» – human rights, environment, pollution control, security, industrial competitiveness – whose importance is growing on the «new security» concept. If the «demand cube» is analyzed, it could be concluded that *new capabilities* get a special importance for the area around the origin (peace-crises, civil decision-making and public-corporate management). By shifting in space and moving towards extreme cube segments, certain elements strengthen that are not too related to concepts of high democracy, individual freedom and civilized society.

The private sector and government cooperation in the area of information exchange should enable privacy and individual rights protection. Exposing personal data to public can cause damage (such as loss of business options or credit rating), but interferences of government institutions can be even more harmful to citizens. In Croatia and in ex-Yugoslavia experiences with government agencies and even with the civil defence systems were perceived very badly in a sense that for many individuals they represented violation of freedom and personal development. Unfortunately, private motives and interests were often in the background for actions against ordinary citizens on behalf of national interests and state security.

Conclusion

The break-up of bipolar structure in power relations resulted in the emergence of new organizations, «players», non-state structures on the local and global scene with unpredictable interests, intentions, dimensions, structure, military and combat power. Today, new asymmetrical threats are caused by military high-tech proliferation, networking and immense growth of information and communication technology usage together with the traditional human ambition in fighting for power and resources, as well as in striving to realize ideological goals.

Therefore, the majority of contemporary traditionally created national SaDS introduce reforms in the area of organizational structure, communication, information system, weapons, education systems, key capabilities, networks and alliances, evaluation and performance measurement in organization, decision making and support for planning and decision making.

Untraditional threats require learning new responses and the precondition for this is the creation of new capabilities, new structures and new methods of management. Successful SaDS must meet criteria of proper function in three main states referring to threat and conflict: peace, crises (low-intensity conflicts), war. Due to complex organizational structure, contemporary organizational SaDS must use in its operation recent solutions from three organizational management paradigms: government (state) sector, military organization, corporative sector. The so-called «demand cube» represents the formal framework for security and defence organizations.

In the information era one shift is made from the islands of «national state» towards the developed society without strict borders, with trans-national entrepreneurial regions, sectoral clusters, individual initiatives (instead of government initiative), companies in foreign ownership. Such a situation renders difficult the government and private sector partnership in matters of security issues and restricts the sovereignty of government (especially military) in the areas of information access, infrastructure and competencies. Indirectly, however, this situation supports civilization achievements in the areas of individual freedom and human rights.

Strategic SWOT analysis for the context of security focuses intensively on the elements of threat and weaknesses of organization. With respect to resource theory concepts, the recommendation for the solution for internal strengthening is found through forming networks and alliances. Internal weaknesses must be overcome by accelerated development of new capabilities from the areas of detection, recognition, protection and non-invasive methods. Attributes of outside threats should be placed in the context of a particular country this threat is directed to for reasons of correct perception and making adequate responses.

References

[1] Čehulić, Lidija: NATO after the Cold War, from the book Grizold, A; Čehulić, L.: International Security and NATO in the New World Order, FPZ, Zagreb 2006, p 93.

[2] Systematic illustration given in various books can be found in: Grant, Robert M.: Contemporary Strategy Analysis, 3rd Edition, Blackwell Publishers Inc., UK, 1998

[3] Kim, Danie H.: The Link between Individual and Organizational Learning, MIT Sloan Management Review, Volume 35. Number 1, fall 1993, Cambridge USA

[4] Nonaka, I. and Takeuchi, H.: The Knowledge-Creating Company- how Japanese Companies Create the Dynamics of Innovation, New York, Oxford University Press, 1995, pp. 4.-36.

[5] «Key competences represent collective learning in an organisation with regard to coordinating different (industrial) skills, work organizations are the result of complex communication processes and knowledge synergy…combination of expert and manager skills from different functional areas.» Hamel,G.; Prahalad, C.K.: *The Core Competence of the Corporation*, Harvard Business Review, May-June 1990., p. 79.-90.

[6] Nye, Joseph: The New Rome Meets the New Barbarians, Economist, 21 March, 2002

[7] Lyon, Rod: Civil-military relations in an Age of Terror, pp 7., www, downloaded on 25.04.2006.

[8] Grizold, A., Tatalović, S., Cvrtila, V.: Modern National Security Systems, FPZ, Zagreb 1999, pp. 9-11

[9] Alvin and Heidi Toffler: War and antiwar, 1993, translation PAIDEIA, pp. 161.-166.

[10] Argyris, C.: Double Loop Learning in Organizations, Harvard Business Review, September-October, 1997, pp. 115-124

[11] Tipurić D. and Fabac R.: "Sustainable Competitiveness- The Impact of Learning on Organizational Capabilities", International Conference of the GBATA, Budapest, July 8-12, 2003; Readings Book: Challenging the Frontiers in Global Business and Technology: Implementation of Changes in Values, Strategy and Policy; pp. 1244-1253, Budapest 2003

[12] «Two concepts are important: “network business strength” (NBS) and “cooperative strength index” (CSI). “ Fabac R.: Cooperation of Competitive Companies of Complementary Resources – Business Strength from the Game Theory Perspective, Ekonomski pregled, br 7/8, pp. 750-769, Zagreb 2002.

[13] Christopher Bennet, NATO Review, April 20 2003, p.6

[14] Diamond, L.: Winning the Cold War on Terrorism: The Democratic-Governance Imperative, Institute for Global Democracy, Policy Paper No. 1, March 2002, pp. 6-7, www, 12.05.2006.

[15] Business Monitor International, Croatia Defence&Security Report Q1 2006, p.16