Damir Črnčec

Pregledni znanstveni članek

IZMENJAVA OBVEŠČEVALNO-VARNOSTNIH IZKUŠENJ Z EVROPSKO UNIJO IN NATOM

EXCHANGE OF EXPERIENCES IN INTELLIGENCE AND SECURITY WITH THE EUROPEAN UNION AND NATO

Review paper

Povzetek Na obveščevalno-varnostnem področju so se s članstvom v Evropski uniji in Natu Sloveniji odprla številna nova vrata, kajti tudi tukaj, tako kot na drugih področjih, smo s svojimi partnerji sedli za isto, skupno mizo. Sodobna obveščevalno-varnostna dejavnost deluje v razmerah nove obveščevalne paradigme, ko je sodelovanje in izmenjavo informacij treba zagotoviti na različnih ravneh znotraj države, kot *intra-* in *inter*resorno, ter zunaj države, dvostransko v EU in Natu ter z OZN, ko gre za udeležbo na mednarodnih operacijah in misijah na taktični in strateški ravni. Dejavnost ni odvisna od hierarhičnosti strukture, temveč je sploščena, deluje horizontalno, saj obveščevalno-varnostne strukture, ki so zelo jasno vpete v organizacijsko strukturo, neposredno podpirajo najvišje odločevalce ter samostojno izmenjujejo obveščevalne informacije med seboj, z državami članicami, poveljstvi Nata itn. Temu ustrezno je treba nadomestiti in nadgraditi načelo potrebe po védenju z načelom potrebe po deliti z (drugimi).

V preteklosti je Nato namenjal varnosti precej več pozornosti kot EU, ki se je reševanja te problematike intenzivno lotila šele po letu 2001. Istega leta je tudi Slovenija postavila normativne temelje sodobnega, primerljivega sistema ravnanja s tajnimi podatki, njegova implementacija pa je nikoli končan proces.

Ključne besede ***Evropska unija, nova obveščevalna paradigma, obveščevalno-varnostna dejavnost, Obveščevalno varnostna služba Ministrstva za obrambo, Slovenska obveščevalno-varnostna agencija, tajni podatki, varnost, zveza Nato.***

Abstract With membership of the European Union and NATO, a number of new doors opened up for Slovenia in the area of intelligence and security. Similarly to other areas, Slovenia sat behind the same table together with its partners. Modern intelligence and security takes place in conditions of new intelligence paradigm, where cooperation and exchange of information should be provided on various national levels, as *intra-* and *inter-*agency activity, and outside the country, bilaterally within the EU and NATO, and with the UN when it is related to participation in international operations and missions on tactical and strategic levels. This activity does not depend on the hierarchy of the structure, but it is flattened and functions horizontally. Intelligence and security structures are namely clearly incorporated in the organizational structure, they directly support top decision-makers and exchange intelligence among themselves autonomously, with member states, NATO commands, etc. In consideration of this, the need-to-know principle should be replaced and upgraded with the need-to-share (with others) principle.

In the past, security was given far more attention within NATO than in the EU, which began to intensify its activity in this area only after the year 2001. In the same year Slovenia also set the normative basis for a modern, comparable system of classified information management, taking into account that its implementation is a never-ending process.

Key words ***European Union, new intelligence paradigm, intelligence and security, Intelligence and Security Service of the Ministry of Defence, Slovene Intelligence and Security Agency, classified information, security, NATO.***

Introduction

International cooperation in the area of intelligence and security has always been part of intelligence and security structures' operations. Since its beginnings, Slovenia has established bilateral intelligence and security relations with individual countries that have or have not been members of the European Union and/or NATO. Following the first democratic elections in the late eighties of the previous century, the intelligence and security, both civilian and defence-military, was directed at preserving Slovenia's independence processes. Given the current information, one can argue that it was a success story of intelligence and security structures of the then republic in the federation.

Approximately a decade ago the process of adjustment to modern standards in the intelligence and security area, and their implementation increased in intensity. This same period also saw the adoption of the modern Police Act in 1998 and the modern Slovene Intelligence and Security Agency Act in 1999, while the Defence Act underwent continued amendments and upgrades after the year 1994. The first two acts were important all the more as they regulated the uniform method of authority used in the past concerning the functioning of intelligence and security structures. Intelligence structures lost their police and executive powers linking intelligence with so-called political police in the past. For Slovenia of that period, the new European standard represented also a symbolic conclusion of the transformation process of intelligence and security structures launched during the first democratic elections. From a normative perspective worthy of special mention is the Classified Information Act developed in the late nineties and adopted in 2001. This act introduced a NATO- and EU-comparable and modern framework for classified information management across the nation.

The aim of this paper is to analyze and highlight the importance of cooperation in the intelligence and security area as one of the major pillars of the intelligence paradigm. Intelligence and security cooperation within NATO and the EU with Slovenia functioning as an equal factor represents an important aspect of intelligence and security support for the countries and both organizations alike. The analysis is derived from key quality methods. An extra added value to the study is the method of direct participant observation as it enables gathering of relevant information from practice. The paper presents subject matter that is rather limited in its essence, since research of intelligence still involves a collision of scientific curiosity and secrecy requirements. A clear overview of modern trends and challenges is given in the context of international cooperation, and a complete and original description is provided about the position of intelligence in NATO and the EU. Particular attention is given to the role of Slovenia's intelligence and security structures *vis-à-vis* NATO and the EU.

When in the early nineties of the previous century Slovenia noted in its key documents that integration into the EU and NATO was its strategic objective, this also applied to intelligence and security. In the first stage it particularly implied more intensive cooperation with member states of the EU and/or NATO. It should be stressed, however, that a considerable part of cooperation evolved also in other branches of power, notably the legislative branch gathering experiences about the implementation of intelligence and security in democracy, but also about its appropriate control. Accession to these two international organizations, which otherwise pursue different missions, but whose legitimacy, at the same time, is based on respect for human rights and basic freedoms, democracy, respect for law and order, and other modern civilization principles, was imperative for Slovenia in order to ensure long-term stability of the country, its citizens and, after all, Slovenians as a nation.

In the continuation of the text some attention will be dedicated to the lessons learned and exchanged from the perspective of classified information management, with intelligence and security structures being incorporated primarily in the preventive aspects of providing security, as for instance security clearance of persons, bodies and organizations, introduction of minimum security standards, etc. Minimum standards in the EU and NATO pertaining to security are very similar and often interoperable. In the past, attention to security within NATO considerably exceeded that of the EU, which intensified its approach to these issues only after the year 2001.

Over the past five years of Slovenia's membership in the EU and NATO, several new doors have opened, as Slovenia, similarly to other areas, here also joined its partners behind the same table. In the EU, cooperation has evolved into presiding over equal partners with Slovenian Presidency of the EU Council in the first half of

2008. Slovenia has progressed to a country that gathers and also offers experiences, i.e. it exchanges them through various forms of cooperation.

More than ever before, and in particular after 11 September 2001, contemporary security environment has been marked by a global and transnational character of threats. A more intensified cooperation among all institutions facing these threats has, therefore, become necessary. The EU and NATO rely on the available intelligence and security capabilities and particularly on intelligence and security support of member states. Consequently, national intelligence and security services and structures of the EU and NATO had to adjust within the framework of a new intelligence paradigm.

1 NEW INTELLIGENCE PARADIGM

A new intelligence paradigm[1] is composed of the most recent trends in this area. There are at least **seven** trends which impact on the nature of intelligence service operations. ***The first*** trend refers to the transformation of national intelligence and other related structures. The most obvious example of this trend is the transformation of the largest intelligence community, i.e. the US intelligence. The aim of the transformation is to ensure better coordination and data evaluation, and their dissemination to users within the shortest time possible. Directly linked with the first is ***the second*** trend which expands the obligations and powers for data-gathering by intelligence services, most often through substantial encroachment on human rights and freedoms. ***The third*** emerging trend is a requirement for intelligence and evidence with forensic value. This trend is posing a whole range of new challenges and requirements to intelligence services. Data obtained through technical means require accurate and quality processing within a very short period of time, finalization to an appropriate evidentiary level (sic!) and then dissemination to clients within the shortest time possible. ***The fourth*** trend is linked with an increased capacity for the transmission of large amounts of data and information, which often makes intelligence services unable to compete with the means designed for transmission of data and information, such as television, radio, internet and telephone calls (conversations, SMS), which represent the most frequent medium for exchanging the news. ***The fifth*** is embedded in the spirit of the flattened, horizontal world. The flattening access and usability of information technology allowed one billion people to use the internet in 2007, although within this billion some individuals may misuse the internet to compromise the achievements brought by the internet itself. ***The sixth*** trend is the result and consequence of the penetration of the third and fourth trends into intelligence community. Intelligence services are required to support strategic, operational and tactical users with relevant intelligence. The contents should be adjusted for use on different levels, taking into account that, in the information age, tactical moves in the theatre or during the execution of intelligence can have strategic implications. ***The seventh*** trend is closely linked with the first, yet it surpasses its sole national dimension. International cooperation in the area of intelligence, among

[1] *More on the new intelligence paradigm in Črnčec, 2009b, p. 83–85.*

countries, and within the framework of various supranational, security, regional or economic organizations has nowadays become more important than ever before. In the continuation of the text, the new paradigm will be addressed mainly from the perspective of intelligence processes at the national and international levels.

The common denominator of all these trends is of course ***man, an individual***[2] possessing appropriate education and qualifications, permanently trained in his area of expertise, as well as in the use of information technology and the protection of human rights and basic freedoms. An individual who understands that the environment around him has changed, that the organization he works for and he himself need to change. Changes should include changing the culture of secrecy that has always been and of course continues to be one of the key guiding principles of intelligence services. It is, therefore, essential that collaboration within, and among organizations, both domestically and internationally, be ensured. The culture of secrecy manifested through the *need to know* principle should be replaced and upgraded appropriately with the *need to share* principle or *responsibility to provide*. It is necessary to allow access to information to a wide circle of institutions that are differently involved in the process of ensuring national security, facilitated through information technology. A joint information network linking all institutions that function either as receivers or originators of information would be a welcome development. In the culture itself, it is not enough to be understood, defined in doctrines and then implemented by intelligence structure. It should be a process directed by and adhered to by the entire intelligence community in the widest sense, including those using intelligence products. These circumstances determined by the new intelligence paradigm could not be avoided neither by nation states nor international organizations, namely NATO and the EU. They will thus be given special attention in the continuation of the text.

2 INTELLIGENCE AND SECURITY IN THE EUROPEAN UNION

The EU is a supranational international organization founded as the European economic community of six countries which became a European organization (community) with 27 member states in 2007.[3] The EU expects and demands from its members to renounce part of their national sovereignty for the benefit of the Union. Despite this, it is understandable that intelligence and security falls within the exclusive competence of member states as one of the key attributes of a modern sovereign state. As already referred to above, the EU and NATO **do not have** an intelligence and security service of their own. There are bodies existing in both organizations dealing with the issues of intelligence, counterintelligence or security. The management of classified information is regulated in detail, while the intelligence and security remains the domain

[2] *The Time magazine chose man as the 'Person of the Year 2006'. An individual is a person mastering the information era and one who both creates and uses information age services, an individual changing the art, politics and trade. A proactive individual is the citizen of the new digital democracy. Time, 25. 12. 2006/1. 1. 2007. The magazine was published in 6,965,000 copies.*

[3] *Following the "big bang", i.e. the integration of ten new members in 2004, the EU expanded in 2007 to the present number of members with the inclusion of Bulgaria and Romania.*

of member states of both organizations. Countries are still unwilling to delegate part of their sovereignty to supranational institutions such as the EU. However, modern threats and security challenges demand new forms and more effective ways of information exchange. The EU addresses these issues both in the second and third pillars[4].

As part of the third pillar, the EU is focused primarily on countering the threat of terrorism. This involves some forms of cooperation dating several decades back. The ***Bern Group or Club*** was established in 1971. It originally involved six European security services, including the British Security Service, French DST, German BfV and Swedish SAPO. The director-level meetings are held twice a year and are not meant to be solely social gatherings. The group incorporates security services from the EU member states. Within the club, there are working subgroups dealing with specific problem areas (terrorism, organized crime). After 11 September 2001, the Bern Club established a new organisation called the ***Counterterrorism Group*** (*CTG*). This is a separate body with a wide range of membership involving EU intelligence and security services, and additionally the services of the US, Switzerland and Norway. The first meeting of CTG was in November 2001. Currently, the most important activity of this group is identification of threats posed by terrorism. Although not under direct jurisdiction of the EU, its analyses of security threats are available to individual high EU committees. CTG has no formal seat, and its presidency rotates together with the EU presidency (Aldrich, 2004).

The ideas of developing some sort of a European version of the US intelligence agency, the CIA, appeared previously within the European Union and tend to emerge during incidents that affect the entire Union. Such an example was the terrorist attacks in Spain in March 2003, which claimed more than 200 deaths and injured 1,500 others. The EU responded quickly and appointed a ***counterterrorism coordinator*** responsible for enhancing cooperation amongst member states, EU working bodies and other relevant entities. The main stress of their role is the exchange of intelligence among member states. Javier Solana, a high-ranking representative of the EU for common foreign and security policy, has proposed that the present Situation Centre of the EU Council, which collects and analyzes information on external risks should do the same in the area of internal security threats. Continued cooperation remains imperative among the countries and their intelligence and security services, as does the efficient exchange of information to allow timely implementation of preventive measures.

As part of the EU second pillar, cooperation among intelligence services depended heavily on bilateral relations. Military intelligence cooperation started as part of the European Security and Defence Policy (ESDP) programme adopted at the Helsinki Summit in 1999. The "intelligence architecture" project presented in Chart 1 stems from the EU Brussels Summit in 1999, when the Policy Planning and Early Warning Unit was created[5]. Between 2000 and 2001, the establishment of the EU Military Staff (EUMS) followed, which comprised an integrated intelligence component. The

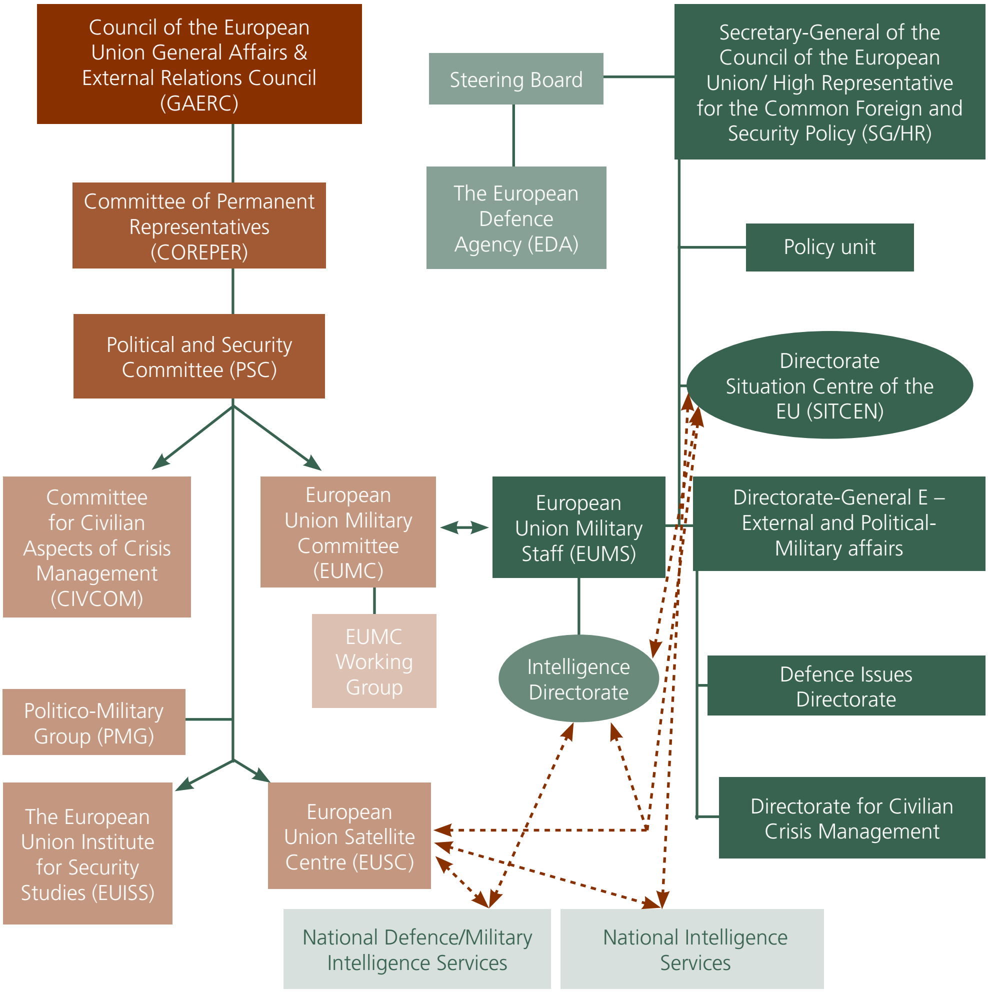
[4] *The second pillar represents the **Common Foreign and Security Policy** (CFSP) and the third pillar the **Police and Judicial Co-operation in Criminal Matters** (PJCC).*

[5] *It is now called the Policy Unit.*

end of 2001 saw the endorsement of the ***ISTAR***[6] concept for EU-led operations. The future challenges of the EU were outlined in the EU Security Strategy entitled "A Sustainable Europe for a Better World". By the beginning of 2007, the development of EU intelligence became recognizable with the creation of common civilian, military, defence and analytical products. The products are made available to all key institutions within the EU and member states.

Chart 1:

Strategic Intelligence Architecture within the civilian and military structure of the European Union


Council of the European Union General Affairs & External Relations Council (GAERC)
Committee of Permanent Representatives (COREPER)
Political and Security Committee (PSC)
Committee for Civilian Aspects of Crisis Management (CIVCOM)
European Union Military Committee (EUMC)
EUMC Working Group
Politico-Military Group (PMG)
The European Union Institute for Security Studies (EUISS)
European Union Satellite Centre (EUSC)
Steering Board
The European Defence Agency (EDA)
Secretary-General of the Council of the European Union/ High Representative for the Common Foreign and Security Policy (SG/HR)
Policy unit
Directorate Situation Centre of the EU (SITCEN)
European Union Military Staff (EUMS)
Directorate-General E – External and Political-Military affairs
Intelligence Directorate
Defence Issues Directorate
Directorate for Civilian Crisis Management
National Defence/Military Intelligence Services
National Intelligence Services

Source: Črnčec, 2009b : 198

[6] *ISTAR is a concept defining full intelligence support to (military) operations. The concept includes Intelligence, Surveillance, Target Acquisition and Reconnaissance. ISTAR is an element of the intelligence cycle and denotes data collection sensors. NATO uses the acronym (J)ISR as a synonim for Joint Intelligence, Surveillance and Reconnaissance.*

As mentioned previously, discussions about the formation of a European CIA are revived occasionally, but the European intelligence agency still remains just an idea. In practice, the provision of a common ESDP led to the creation of some institutions that dealt with the complete intelligence cycle or individual parts of it. The only real EU intelligence capability is the ***Satellite Centre (EUSC)***[7]. EUSC is an important and proven asset that provides support to EU missions and geospatial products to member states that are the result of the analysis of satellite images and other data. EUSC plays an important role in ESDP by providing analysis of satellite imagery which can be essential for the success of military missions and the safety of military personnel. EUSC priorities are derived from the European security strategy and include: monitoring of regional conflicts, threats by organized crime, terrorism and proliferation of weapons of mass destruction. It has also provided full support for EU operations in Bosnia and Herzegovina and the Democratic Republic of the Congo. Moreover, it is an important early warning tool as it simplifies information-gathering for the prevention of armed conflicts. EUSC can also be guided by EU member states, and it commonly prepares documents for various international organizations, in particular for the UN[8]. EUSC users can be divided into five groups[9]:

- *EU Council and its bodies* – have direct relations mostly with the DG E VIII Directorate, EU Military Staff and the Situation Centre (SITCEN). In accomplishing these tasks, EUSC provided support to 15 different EU missions ranging from PROXIMA in Macedonia to MONUC in Congo. It is highly probable that it will support two important EU missions launched in the first half of 2008, i.e. EUFOR Chad and EULEX Kosovo;
- With 27 *member states,* EUSC cooperates with various working groups and has expert exchange and internship programmes;
- *The EU Commission* may request from EUSC products and services, and cooperates with the centre in joint research projects;
- *Non-members of the EU* (Iceland, Norway, Turkey and EU accession members) can request and receive products, and can also be involved in the direct implementation of EUSC tasks;
- *International organizations,* for instance various bodies of the United Nations Organization, are important partners of the EU in crisis management and conflict prevention. Therefore, EUSC has close cooperation with, and provides support to, the following UN bodies and operations: MONUC (operation in Congo), UNDOF (operation in the Golan Heights), UNDPKO (operation in Sudan - Darfur), UNMIK (Kosovo) and UNMOVIC (Iraq).

Within the EU structure, EUSC provides its products primarily to two bodies dealing with intelligence support of EU operations: the intelligence component of the EU

[7] *More on www.eusc.europa.eu.*

[8] *EUFOR RD CONGO (DRC): The EU Satellite Centre (EUSC) in support of EU operations in the DRC, European Security and Defence Policy (ESDP), January 2007.*

[9] *http://www.eusc.europa.eu/index.php?option=com_content&task=view&id=7&Itemid=15, 6. 3. 2008.*

Military Staff in defence and military areas and the ***Joint Situation Centre***[10] ***(SITCEN)*** of the EU in the civilian sphere. Both structures are heavily supported by EU member states, the defence/military resources of the Military Staff and the civilian resources of the Situation Centre. National contributions are primarily of human resources, whereas the *input* of products is ensured with the help of national representatives functioning under a »*dual-hatted*«[11] role. On the one hand, they are an integral element of the permanent EU structure and accomplish their tasks in accordance with job descriptions defined for individual positions. On the other hand, they also function as national representatives, and points of contact[12] responsible for uninterrupted exchange of national intelligence products between the EU and their own countries. Solutions of this type are particularly practical for small countries with limited human resources, and also useful for crisis response operations both within the EU and NATO.

In terms of formal hierarchical subordination, EUMS and the Joint SITCEN belong to the General Secretariat (GS) rather than the European Commission[13]. For the sake of efficiency, and due to the scarcity of intelligence resources, the High Representative of the GS established the ***Single Intelligence Analysis Capacity***[14] ***(SIAC)*** in 2006. The basic aim of this initiative is to provide all members of the European Union with the best possible analytical product, generated from all available resources and through the cooperation of the Joint Situation Centre and the intelligence component of EUMS. SIAC is jointly led and guided by the Director General of the EUMS and the Director of SITCEN.

There is an emphasis on combining processes as opposed to organizational structures, which of course does not mean that the upgrading of processes and their optimisation will not result in one structure. Harmonized joint products are then also distributed to lower levels. Coordinated analytical products are put on a list with clearly indicated tasking and supporting authorities. The responsible authority for SIAC products, in case of military and defence issues is, naturally, the EUMS ***Intelligence Directorate***.

With intensified activity of the EU during international operations and missions, the EU Commands responsible for individual operations have a greater need for tactical and operational-security intelligence[15]. Such an example, in 2008 and 2009, was EUFOR Chad, which is under the command of the Paris Operation Headquarters. The provision of appropriate permanent intelligence support is one of the key challenges

[10] *When Henry Kissinger was the US State Secretary, he approached the EU with a question about the essence of the EU. The EU had no clearly defined representative or, as he put it, did not have a single telephone number. Joint SITCEN is now the single EU telephone number.*

[11] *POC (point of contact) can also refer to liaison officers involved in the exchange of information.*

[12] *The Commission employs approximately 27,000 employees, the Secretariat around 3,300 and EUMS some 200 employees.*

[13] *The Single Intelligence Analysis Capacity has been in operation since 1 January 2007. All products are produced in accordance with a 6-month programme which is jointly approved by both superiors.*

[14] *For more on intelligence and security support of international operations and missions see at Črnčec 2009a.*

[15] *The Strategic Concept, first published in 1991 and revised in 1999. On 7 July 2009, NATO formally launched the process leading to the new Strategic Concept of the Alliance at a major security conference in Brussels (see http://www.nato.int/strategic-concept/index.html).*

of every international operation and mission. This trend, particularly in relation to defence and military considerations, will lead to even more intensified cooperation in relations between EU member states. If appropriate mechanisms for cooperation and exchange of information are properly established at a strategic level, the EU will definitely continue upgrading direct support capabilities for crisis response operations. An important role in this process is also being played by the European Defence Agency that is developing relevant intelligence capabilities.

The appropriate placement of intelligence structures within the secretariat organization is also important. EUMS occupies the top position in the hierarchy of organizational structures, similarly to the status of directorate-general. Its internal organizational structures, including intelligence, were not given sufficient status. In the structure, effective from March 2008, the Intelligence Directorate within EUMS is led by the director of the EUMS Intelligence Directorate. This appears to show that, in the future, specific attention will be given to strengthening the defence and military intelligence capabilities of the EU. The increased involvement of the EU in international operations and missions highlights a greater practical need for the provision of appropriate intelligence support at operational and tactical levels. In order to provide such support, every intelligence structure needs a clearly defined organizational structure and their own capabilities for collecting and processing data and information. Capabilities should be provided both in the civilian and defence and military areas, for successful and efficient exchange of information will always be a challenge for all intelligence structures and its professionals.

3 INTELLIGENCE AND SECURITY IN NATO

In contrast to the EU, NATO is not a supranational but a defence and political organisation that, as a counter balance to the former Warsaw Pact, has nearly accomplished its historical mission already. In the changed international security environment of the 21st century, the Alliance has taken on renewed significance and, in any case, remains a major factor in providing defence and security of the European Union and the European continent, as well as functions as the bridge for Euro-Atlantic partnership with the US and Canada.

In accordance with the North Atlantic Treaty, NATO is an organization whose main task is to safeguard the freedom and security of its members by political and military means. NATO is an alliance of 28 countries that are equal and sovereign in their decisions. It is committed to defending its member countries against any aggression or threat of aggression in compliance with the principle that *an armed attack against one member is considered as an armed attack against all*. Article 5 of the Washington Treaty was first used after the terrorist attacks on the US on 11 September 2001 when NATO provided assistance to the US. The Strategic Concept[16] stipulates that NATO is committed not only to collective defence, but also to peace and stability of the

[16] NATO Handbook is an excellent source of information about NATO with detailed descriptions of the decision-making process in the alliance, its structures, role in contemporary security environment, etc.

wider Euro Atlantic area. This broad definition of security acknowledges the importance of political, economic, social and environmental factors as a supplement to the defence dimension (NATO, 2006)[17].

Our own and other people's security cannot be provided without an appropriate intelligence and security support. NATO does not have an intelligence service of its own but structures charged with intelligence and security support at various levels, and relies increasingly on the input/contribution of intelligence services of its member states. Intelligence is one of the key factors for successful planning and crisis response. The perception of the necessary intelligence support is also evident from the tasking list of some structures within NATO HQ at Brussels or both strategic commands.

At the Istanbul Summit in June 2004, heads of states and governments of the Alliance agreed, among other things, to the development of high-tech capabilities for the protection of civilians and military forces against terrorist attacks. These assets are mainly of preventive and protective nature. The agreement also includes improvements to the exchange of intelligence and revision of the existing NATO intelligence structures. The mandate of the ***Terrorist Threat Intelligence Unit (TTIU)*** established after the 11 September attacks has become permanent. The heads also agreed that the Alliance should strengthen its support capabilities for the countries facing terrorist threats. The ***Intelligence Liaison Unit (ILU)*** is a special capability closely linked with TTIU that has considerably improved the exchange of the relevant information. ILU is intended for the exchange of intelligence on counterterrorist activity between NATO and Partnership for Peace countries, and since March 2003 also the Mediterranean Dialogue countries[18].

NATO Headquarters is the political "command" of the Alliance located in Brussels, and includes the Secretary General, national delegations, International Staff (IS) and International Military Staff (IMS). The Secretary General has the role of the superior for the "civilian" part of the International Staff, while the International Military Staff reports to the Military Committee. Its chairman is subordinate to the North Atlantic Council (NAC) and acts as a superior to the International Military Staff. Intelligence elements or structures are embedded in both staffs and strategic commands[19].

[17] *See Report on the Partnership Action Plan Against Terrorism, 23. 6. 2004, at http://www.nato.int/docu/basictxt/b040623be.htm.*

[18] *The name of the command located in Mons, Belgium, is the Allied Command Operations (ACO). Its commander is the Supreme Allied Commander Operations (SACEUR). The commander is still referred to with an old abbreviation stemming from the period when he eventually acted as the supreme commander for Europe before the latest transformation of NATO command structure. A more appropriate term would now be the allied commander for (NATO-led) operations as in fact he is the supreme commander of all NATO operational capabilities. Another strategic command is the Allied Command Transformation (ACT), located in Norfolk, Virginia, USA, and is commanded by the Supreme Allied Commander Transformation (SACT).*

[19] *In September 2006 Slovenia held an informal meeting of NATO ministers in Portorož. The meeting was a demanding task for the Ministry of Defence, particularly in terms of logistics and security. Security activities were coordinated at the national level within the secretariat of the National Security Council. The MoD appointed a special group to ensure comprehensive preparation for the event. Its assistant head also acted as assistant to OVS director general, who coordinated all relevant "out" (police, SOVA, NATO) and "in" (MoD, Slovenian Armed Forces, military police) activities.*

The International Staff also includes a special office responsible for coordination and implementation of the Alliance security standards. The office deals with security matters for the Alliance headquarters, coordination of NATO security operations with member and partner countries, the Mediterranean Dialogue countries and NATO civilian and military bodies, implementation of NATO security policy, security intelligence measures and intelligence threats (NATO 2006: 83–84).

NATO Office of Security (NOS) has three main tasks: political control, security (counterintelligence) area and preventive security. As part of the first task of political control, inspections and visits to member states, NATO bodies and all others with access to NATO classified information verify the appropriacy of measures and management of data, and accredited communications and information systems. Security policy, directives, guidance and support in the area of security are approved at the level of ***NATO Security Committee (NSC)*** and NAC, if required. In the area of security NOS deals with counterintelligence policy and control within NATO, and together with TTIU collects information about potential threats to the North Atlantic Council and other key decision-making bodies, including the Military Committee. Similarly to the secretariat, it provides support to the operations of ***NATO Special Committee*** and carries out special security investigations and investigations related to espionage. Preventive security involves activities, such as coordination of protective security programmes and operations, including physical, personal and information security of NATO HQ, consultation for new NATO commands, coordination of security measures for NATO Ministerials[20] and other high-ranking meetings, awareness programmes for users, and response measures for attempts of unauthorized access to computer networks, and other computer-related security incidents.

The key security intelligence structure in the military part of NATO is ***Allied Command Counter Intelligence (ACCI)*** as the sole organic unit of NATO designated for security intelligence. The command is located at SHAPE. Its staff also provides security intelligence support to commanders of crisis response operations[21]. The command is tasked with detection, deterrence and neutralisation of terrorist threats, espionage, sabotage and subversive operations directed against NATO personnel[22]. The command can be manned with representatives of all member states. It provides security intelligence support to all NATO units, commands and personnel of the Alliance and member states.

An analysis of the civilian part of NATO that is considerably smaller than the military structure in terms of size reveals that intelligence and security areas concentrate mainly on security and security intelligence issues, yet to a different extent given the individual area. Intelligence is involved mostly in the provision of information for

[20] *Instead of the term international operations and missions (IOM), NATO uses a narrower term crisis response operations (CRO).*

[21] *See What is ACCI and why should you care?, Kfor Chronicle, Aug 2007, p. 28–29, at http://www.nato.int/kfor/chronicle/2007/chronicle_08/chronicle_08.pdf, 25. 12. 2008.*

[22] *This function is supported through the **NATO Intelligence Warning System (NIWS).** Owing to the need for early warning of the Alliance about imminent threats, NIWS is considered as one of the new intelligence tools of the Post-Cold War period (Kriendler, 2002).*

TTIU and economy-related intelligence. However, the following text will show that intelligence support system is in place for the Military Committee and both strategic commanders within the military structure at the level of the International Military Staff and strategic commands. At the same time, additional intelligence capabilities are being developed in line with the guidelines of the Istanbul Summit and in response to addressing new, modern security challenges and providing intelligence support to NATO units in crisis response operations.

A constituent element of the International Military Staff is the ***Intelligence Division***, which is responsible for day-to-day strategic intelligence support of the Secretary General, North Atlantic Council, Defence Planning Committee, Military Committee and other NATO committees and bodies, as for instance other parts of the International Military Staff, Political Committee, etc. In carrying out its activity, the division relies on intelligence *input* of member states and NATO commands, for it has no capabilities of its own. Based on the gathered information it functions as the central coordination body responsible for collection, evaluation and dissemination of intelligence products within NATO HQ, its commands, agencies, organizations and states. Along with the provision of routine intelligence staff support, the Intelligence Division also develops and coordinates NATO strategic intelligence assessments, guiding and conceptual intelligence documents and basic intelligence documents, and manages selected databases and digital information. Moreover, it is involved in force planning, strategic warning[23] and crisis management, and functions as the contact point for intelligence affairs within NATO and among the responsible national structures. The Division is the key body providing direct intelligence support to all major institutions within NATO and the Military Committee in the development of military advice for political decisions. It is composed of three sections: the evaluation section, the intelligence and warning section, and the section for product publishing and intelligence structures[24].

The ***Situation Centre*** (SITCEN), a component of the International Military Staff, has some intelligence tasks, mainly related to uninterrupted monitoring of global situation and with a focus on operational areas of NATO forces. SITCEN functions 24 hours a day as the central point for the reception, exchange and dissemination of political, military and economic information of interest to the Alliance and member states. It also plays an important role in crisis situations and times of tension, and reports about its operations directly to the political structure of NATO, and assistant secretary general for defence planning and operations. It receives daily guidelines for the implementation of routine tasks from the director of the International Military Staff[25].

Within the framework of strategic commands, ACO provides intelligence support to operational planning and operations, whereas ACT conducts long-term analyses of trends, develops intelligence concepts and capabilities, and is in charge of

[23] *NATO, 2001, p. 525.*

[24] *NATO, 2001, p. 244.*

[25] *See NATO School Oberammergau, at http://www.natoschool.nato.int/.*

education[26]. A similar division of responsibility is used in the field of communications and information systems. In accordance with the established command structure, intelligence support to planning and operations is delegated from ACO to three operational or joint commands [27].

In line with commitments adopted at the Prague Summit in December 2002, the Military Committee supported the establishment of ***Intelligence Fusion Centre (IFC)***[28]. Its purpose is to ensure transmission of useful, time-relevant (real time) and accurate military intelligence and information crucial to support planning and execution of NATO-led operations. IFC represents an important capacity distributing global intelligence among the member and partner countries of the Alliance and thus improves direct intelligence support to ACO. Its purpose is to provide comprehensive intelligence from all sources in support of NATO-led operations. The establishment of IFC is yet another method of responding to security challenges of the 21st century. IFC was officially launched on 16 October 2006[29]. The US provides logistic support for the centre in Molesworth, in the United Kingdom. Manpower plans foresee 160 experts from all NATO member states[30].

Intelligence and security channels in NATO are closely intertwined. There is a clearly expressed two-way role of member countries providing their *inputs* to be able to utilize the upgraded results. The essence of all processes is that they enable access to all required data to key players within NATO. The awareness of the altered security circumstances in the aftermath of 11 September demanded that the Alliance provide an even faster flow of all the relevant intelligence and security data and upgrade them as well, on strategic and operational levels alike. Undoubtedly, a suitable information and communications infrastructure is of course a precondition for this. This role has been predestined for the IFC which became a fact during the past three years, while the TTIU is becoming and remains a strategic capability of the Alliance, specialised in the field of terrorism. Considering that NATO is a politico-military organisation, the role of military (defence) intelligence and security services is correspondingly more emphasised as far as intelligence support is concerned. Namely, these services directly

[26] *ACO has the following subordinate commands: Joint Force Command in Brussels, Joint Force Command in Naples and Joint Headquarters Lisbon.*

[27] *IFC is an organization outside permanent NATO structure and is designated for ACO support, primarily in providing intelligence support for NATO Response Forces), allied forces with top-level equipment that are deployable to any area if required. Throughout development, IFC, role has become significant in the provision of intelligence support, mainly to allied crisis response operations.*

[28] *See Launch of the Intelligence Fusion Centre in Support of NATO, Global Intelligence Assesment for NATO Countries, www.nato.int/shape.*

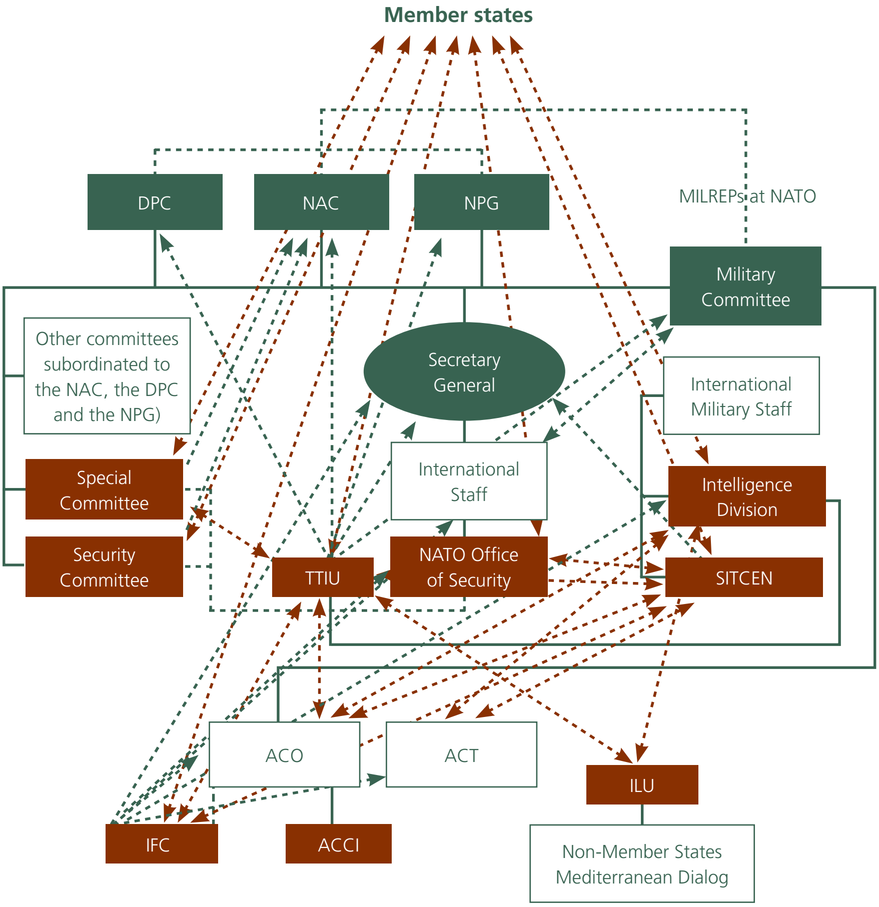
[29] *New NATO Intelligence Center Opens in Britain, www.britainusa.com.*

[30] *From 28.5.2009 to 29.5.2009 the spring conference of directors of defence intelligence services of NATO member states (NIB – NATO Intelligence Board) was held in Brdo pri Kranju, Slovenia. The conference was chaired by Ms Karen A. Laino, AD IMS for Intelligence. Conference participants were also addressed by the Minister of Defence of the Republic of Slovenia, Ms Ljubica Jelušič, who emphasized the importance of work of intelligence services in support and protection of armed forces troops participating in international operations and missions and in support of the highest decision-makers as well as the importance of intelligence exchange and cooperation between the intelligence services. See http://www.mors.si/index.php?id=novica&L=1&tx_ttnews[tt_news]=1518&tx_ttnews[backPid]=1&cHash=2acd998ffd*

support the key strategic body – the Intelligence Division. Directors of these services meet periodically and regularly with the head of Intelligence Division and ***Assistant Director Intelligence (AD INT)*** and they do so within the ***NATO Intelligence Board (NIB)****31*. Also, these services fill in the intelligence gaps at different levels, including the most important strategic-operative intelligence structure, the IFC. Chart 2 shows that intelligence support is not tied to some hierarchical nature of the structure but is rather flattened, i.e., operates horizontally, as intelligence structures, which are very clearly inserted into the organisational structure, directly support the highest echelons of decision-makers and independently exchange intelligence among themselves, the member states, NATO commands, etc.

Chart 2:

Strategic Intelligence and Security Architecture within the NATO Civilian and Military Structures



Source: Črnčec, 2009b : 205

[31] *In 2004, AC 46 was chaired by Denmark. In 2008, doubts appeared in the media about the appropriacy of Hungarian presidency, as the director of the responsible Hungarian service had been trained in the Soviet Union. In December 2007, the national security office was taken over by the new director Sandor Laborc, who had been trained at the KGB Academy Dzeržinski. Despite the articles in the media and numerous speculations, Hungary did not decide for his replacement, and none of the member countries demanded this officially. The presidency was then handed over to Iceland.*

On the other hand, civil intelligence and security services are more incorporated in security - counterintelligence carried out in a smaller, civilian part of NATO HQ and involved in counterterrorism. The civilian structure also includes ***NATO Special Committee*** (also referred to as ***AC 46***), which is "among other things responsible for the adoption of internal security measures in member states. Its chairman in the early 1970s was Günther Nollau, the head of federal office for the protection of constitutional order" of the time (Schultz 2001: 45). The Special Committee acts as the key advisory body to the North Atlantic Council on the issue of espionage and terrorist threats to the alliance. It functions at the level of directors (general) of intelligence and security services, with the presidency rotating among member countries. The committee represents one of the most senior NATO working bodies in charge of routine matters, such as security clearance and cryptography. In fact it accomplished a significant role during the accession period of new membership candidates. Along with NOS, the advisory committee exerted pressure on the candidates to "remove" those persons from intelligence and security services that were (had been) under the influence of Russian intelligence services (Aldrich 747: 2004)[32]. Comprehensive support to the operations of the Advisory Committee and the Security Committee is provided by NOS, and its director is the chairman of the Security Committee as well□. This committee functions as the advisory body to NAC from the viewpoint of security policy that is well-developed within NATO. The Security Committee is composed of national representatives, national security experts and security experts from NATO civilian and military structures. At the same time, counterintelligence within various NATO commands and for NATO staff falls within the competence of national military (defence) counterintelligence structures cooperating closely with NATO counterintelligence structure.

NATO has a clear mission. In order to provide intelligence support to the mission, the strategic system is fully appropriate to provide this support, notably following the establishment of IFC. It the mission spreads more to the "civilian" sphere, it may be reasonable also to think in that direction. Room for the improvement of NATO intelligence support is definitely on the operational and tactical levels, mostly in support of allied operations.

Following 11 September, NATO took first steps on the basis of the Prague and Istanbul Summit guidelines to improve intelligence and security architecture. Since security policy remains one of the key areas for efficient and secure operations of the alliance, it also received appropriate attention in the past. The intelligence aspect was in urgent need of development momentum toward IFC as its cornerstone. It is of course premature to think that this may be the very beginning of NATO intelligence service. The military sphere definitely shares a common interest for joint activity in crisis response operations, where everybody is confronted with collective threats to their own service members, which would press on military (defence) services for more intensive cooperation and exchange of information at the tactical and operatio-

[32] *NATO 2006: 134*

nal (in crisis response operations) and strategic levels. Also in the future, cooperation will progress in the same direction.

The knowledge about the principal importance of the political-security and military dimension does not suggest that the economic aspect is being neglected, quite the opposite. Economic threats are part of the complex notion of the 1999 security concept. Economic and financial dimensions of terrorism are high on priority list. Based on the contributions of member states for NAC, the capitals of member states and military bodies are constantly harmonizing assessments of economic intelligence issues (NATO, 2006: 57). In consideration of the intensity of the global crisis in 2009, it can be expected that economic intelligence and security issues will attract even more attention in the future, both in NATO, the EU and other countries.

4 EXCHANGE OF EXPERIENCES IN INTELLIGENCE AND SECURITY AREAS

There are two intelligence and security services in Slovenia: the ***Intelligence and Security Service*** of the Ministry of Defence (OVS) and the ***Slovenian Intelligence and Security Agency*** (SOVA)[33]. Both of them perform intelligence, counterintelligence and security, with the key resposibilities of SOVA being the field of national security and of OVS the field of defence. The SOVA personnel are empowered to undertake special forms of data collection, but have no police authority, while OVS personnel involved in intelligence and counterintelligence have the same powers as SOVA personnel, and the security personnel of the OVS have police powers. Simultaneous use of both types of powers is of course forbidden. Historically speaking, they are two totally different services. SOVA is the successor to the Security and Information Service (VIS), which succeeded the National Security Service (SDV) or political police[34] that functioned in Slovenia up to the introduction of a multi-party system[35]. The OVS was established only after the first democratic elections in April 1990.

During the 1990s, Slovenia revised the legal framework for the operation of security and intelligence structures. The modern and democratic normative basis has facilitated integration into intelligence and security structures and processes in the EU and NATO.

[33] *In Slovene Obveščevalno varnostna služba Ministrstva za obrambo (OVS) in Slovenska obveščevalno-varnostna agencija (SOVA).*

[34] *Still in 1990, when the Federal Secretary for Internal Affairs determined in the Rules on Operations of the National Security Service (SDV) the methods to be used by SDV concerning human rights of the citizens. Without any prior court approval it was allowed to carry out secret eavesdropping, secret control of telephones and other telecommunication means, international and other telecommunications traffic, mail and other shipments, secret recording and document management, technical checks and protection of premises and facilities, secret searches of premises, and maintenance of secret liaison with co-workers. The measures were carried out temporarily or permanently.*

[35] *For more on the activity of the National Security Service and the Security and Information Service in the period before, during and after Slovenian independence see Brejc 1994.*

Hence, there has been no great need for Slovenia to modify its national security system or the structure of its intelligence services after 11 September 2001. I would particularly like to stress that Slovenia, unlike some other countries, has not succumbed to the temptation of strengthening its counterterrorism legislation although terrorism in Slovenia remains a security threat and a criminal act. Intelligence services are primarily the first authority to detect or perceive terrorist threats. Should these threats be real and imminent, they are required to submit such information to potentially affected parties, the police and other bodies within the national security system.

4.1 Exchange of experiences and the European Union

With the adoption of the Classified Information Act in 2001 and the relevant amendments and changes in the next years, Slovenia set up the system of classified information management that is compatible with EU and NATO standards. Five years of experience deriving from the EU membership confirmed and highlighted the issue that despite the progress in the past years, the field of security in the EU is still less developed than that of NATO. Slovenia can make contributions to the development of this area by giving proposals and initiatives for the upgrading of the system of classified information management.

In intelligence, Slovenia has been a full partner of EUSC since 2004. The representative of the MoD is the national representative and member of the managing committee. EUSC provides Slovenia with its products on compact discs and DVDs kept in a special digital library of the MoD. Part of mainly more current products is also accessible through the EUSC web portal where the products are protected with the Chiasmus code key (Florjanc, Ilnikar, 2007: 19). EUSC is a highly usable capability, particularly for smaller countries. During the EU Council Presidency, Slovenia was the first presiding country to activate EUSC for the EU and, hence, caused a precedent.

EUSC is an important institution for the provision of intelligence and security support to international operations and missions of the EU. In 2008 and 2009, such an example was EUFOR in Chad commanded by the operational command in Paris. The establishment of appropriate and permanent intelligence and security support remains one of the key challenges for every international operation and mission. Slovenia ensured this support through bilateral links and assignment of intelligence officers to commands. Good knowledge of intelligence and security processes, part of which are also responsible Slovenian institutions, constitute an important contribution to the provision of adequate intelligence and security support.

Against such background knowledge of the modern security environment, Slovenian security and intelligence structures conducted preparations for the presidency of the Council of the European Union in the first half of 2008. During the presidency, both services gained first-hand experience of the international environment. During the presidency, SOVA organized three events related to its area of work in Slovenia. The Security and Intelligence Service of the Ministry of Defence hosted the second workshop on intelligence and security support in crisis response operations, focusing on Operation EUFOR in Chad[36].

During the preparations for and the actual presidency of the Council of the European Union, both agencies intensified the exchange of intelligence data and products, both domestically as well as with foreign partner services and international organizations. The agencies were faced with additional responsibility, namely, by potentially submitting wrong assessments and information they could risk immediate reaction not only at the national level, but also at the level of the EU. The provision of intelligence and security support for national decision-makers and at the same time the presiding EU Council also constituted **direct** intelligence support for the EU.

4.2 Exchange of experiences and NATO

The system of classified information management in NATO has set the basic framework for the establishment of a modern system of classified information management since the end of the 1990s. Security-related experiences were transferred to responsible Slovenian institutions through NATO inspections that visited Slovenia during its accession period. It should be stressed that the experiences flowed in both directions, and some Slovenian solutions were also implemented in NATO later on. For example, a considerable number of Slovenian functionaries were exempt from security clearance procedures for the access to classified information. Naturally, Slovenia is not the only exception in this case. Yet through the documents adopted in 2008 NATO enabled such a solution also for the classified information of the alliance in compliance with the national regulation of member states.

Immediately upon its accession to NATO, Slovenia filled up some intelligence and security duties in NATO structures. In operations conducted under the auspices of NATO, for instance IFOR and SFOR, it also manned similar positions, but with limited access to classified information. This restriction was of course removed after 2004.

Similarly, after 2004 Slovenia became active within the framework of the Act on the Prevention of Money Laundering and Financing of Terrorism, both in providing protection for commands and in crisis response operations. In accordance with the decision of the RS Government, Slovenia has also become involved in IFC, with maximum two defence military experts. Participation of Slovenia in IFC is an important contribution as it involves continuation of participation in NATO intelligence structures and exchange of intelligence and security information, providing significant support to NATO-led operations and activity of the Alliance response forces. Detailed operation of the centre was regulated through a Memorandum of Understanding[37].

[36] *See Report of the Slovenian EU Council Presidency, 2008.*

[37] *Press release about the decisions adopted by the RS Government at its 88th session, on 14 September 2006, p. 15–16, and the decision of the RS Government granting authority to OVS director general for the signing of the Memorandum of Understanding.*

A precondition for this was surely an appropriate information and communications infrastructure. This was exactly what Slovenia, and in particular defence-related intelligence and security, gained with NATO membership. With the signature of the 2004 Memorandum of Understanding on the establishment of the organization structure for the introduction and operation of the battlefield information collection and exploitation systems, the Republic of Slovenia obtained the right to establish links with the *Battlefield Information Collection and Exploitation Systems (BICES*) and other NATO information networks. During this period, BICES has proved as one of the major sources and a key means for the exchange of intelligence in NATO[38]. The present memorandum expired at the end of February 2006 and was superseded by a Memorandum of Understanding, with the basic element being the adequately amended document of NATO system organization for battlefield information collection and exploitation[39].

Conclusion

The European Union and NATO have several bodies, committees and subcommittees tasked with policy adoption and implementation. Security is an area given special attention in both organizations, and, referred to as "*The issue"* in NATO, the key area enabling successful operation of both organizations.

Modern time requires a modern way of addressing the full range of risks and threats. In intelligence, this can only be possible *first*, with the new intelligence paradigm. The new intelligence paradigm, an important part of which involves active cooperation among intelligence and security structures, is something Slovenia cannot avoid as an active member of NATO and the EU, and a full partner in intelligence. *Second*, given the fact, that both the EU and NATO have no intelligence service of their own, the role of individual member states is so more important. The national intelligence system should be properly structured and organized in order to provide optimum support for intelligence capabilities of both organizations, but also to efficiently receive intelligence products. It is, therefore, reasonable and rational to upgrade the national intelligence system through better transparency and use of available resources. *Third*, in the period of modern transnational threats, cooperation and exchange of information should be ensured at various levels within the country, as *intra-* and *inter-agency*, and bilaterally outside the country, within the EU and NATO, and with the UN, concerning participation in international operations and missions at the tactical and strategic levels. The need for division considerably exceeds national dimensions and has, long ago, become a supranational need of all actively involved in international security environment.

Fourth, modern intelligence and security support is not dependent upon the structure hierarchy, but it is ***flattened*** and functions horizontally, as intelligence and security

[38] *BICES is managed and maintained by NATO BICES Agency, owned by member countries.*

[39] *Press release about the decisions adopted by the RS Government at its 59th session on 2 February 2006, p. 10, and the decision of the RS Government granting authority to OVS director general for the signing of the memorandum.*

structures that are clearly embedded in the organization structure carry out direct support to top decision-makers and autonomous exchange of intelligence among themselves, with member states, NATO commands, etc. The principle of the ***need to know*** should be replaced and upgraded appropriately in line with the principle of the ***need to share***. Within the framework of a special strategy[40], the principle of the need to share should be upgraded to a new mind framework, a concept encompassing its full implementation according to the principle of ***responsibility to provide***. A wider circle of institutions involved in national security should be given access to information through information technology. A collective information network linking all the institutions receiving or generating information would be a welcome innovation. In itself it is insufficient for this new culture to be understood, defined in doctrines and implemented solely by intelligence structures. It should rather be a process guided and adhered to by the entire intelligence community in the widest sense of meaning, including the users of intelligence products that are harmonized, guided or controlled by intelligence services.

Finally, it can be expected that intelligence and security capabilities of the EU and NATO will be built up also in the future. The integration of intelligence and security processes will surely enhance, and may at the same time lead to integration of parts of intelligence and security structures. The final goal remains, nevertheless, unchanged – to provide the best intelligence and security support to all EU and NATO users. Considering the progress of the past years it should not be forgotten that we are still a long way from a "European or NATO" intelligence service functioning as national intelligence services. During its five years of membership in both establishments and a decade of experience exchange, Slovenia has demonstrated and proved several times that membership of intelligence and security structures should be understood as a two-way process, involving the principle of both give and take. Sitting behind the same table that Slovenia chaired as *primus inter pares* can only confirm our self-confidence that the exchange of experiences has been and will be understood also in the future as a commitment and responsibility to our current and future partners.

Bibliography

1. *Aldrich, R., J., 2004. Transatlantic intelligence and security cooperation. International Affairs, 80 (4), str. 731–753.*
2. *Črnčec, D., 2009a. Obveščevalno-varnostna podpora mednarodnim operacijam in misijam. Posvet o sodelovanju Republike Slovenije v mednarodnih operacijah in misijah. Brdo pri Kranju, 21. januar 2009. http://www.mors.si/fileadmin/mors/pdf/sporocila/2009/Obvescevalno_varnostna_podpora_Crncec.pdf, 2. 2. 2009.*
3. *Črnčec, D., 2009b. Obveščevalna dejavnost v javnem informacijski dobi. Ljubljana, Defensor.*
4. *Florjanc, A., Ilnikar, J., 2007. Izobraževanje s področja slikovnih obveščevalnih podatkov. Slovenska vojska, XV/17, str. 19–21.*

[40] *See Information Sharing Strategy at http://www.dni.gov/reports/IC_Information_Sharing_Strategy.pdf., 20. 12. 2008.*

5. *Kriendler, J., 2002. Anticipating crises. Nato Review, Winter 2002. http://www.nato.int/docu/review/2002/issue4/english/art4.html, 15. 2. 2008.*
6. *Schultz, E. H., 2001. Wie der Terrorismus bekämpft wird. http://www.vegesack.de:8080/kunden/schultz/down/1056191578/TerrorBekaempfung.pdf, 20. 12. 2007.*
7. *EUFOR RD CONGO: The EU Satellite Centre (EUSC) in support of EU operations in the DRC (2007). European Security and Defence Policy (ESDP).*
8. *NATO, 2001 in 2006. NATO Handbook. Brussels, Belgium: Public Diplomacy Division, NATO.*
9. *Poročilo o predsedovanju Slovenije Svetu EU, 2008. http://www.svez.gov.si/fileadmin/svez.gov.si/pageuploads/docs/predsedovanje _eu/ 03-07_Porocilo_predsedovanje2008-6_SPREJETO_NA_VLADI.pdf, 23. 12. 2008.*