



Organization for Security and Co-operation in Europe

Report by the OSCE Secretary General

on the Implementation of MC.DEC/2/09

on Further OSCE Efforts to Address Transnational Threats and
Challenges to Security and Stability

Vienna, 11 June 2010

INDEX

INTRODUCTION:	5
<u>PART 1: THEMATIC CASE STUDIES</u>	8
1 - PREVENTING AND COMBATING TERRORISM	8
I. Background.....	8
II. Current Activities.....	9
III. Co-operation with International Organizations	11
IV. Gaps and the Ways to Address Them.....	12
V. Future Activities.....	13
2 - FIGHTING ORGANIZED CRIME	15
I. Background.....	15
II. Current Activities.....	16
III. Co-operation with International Organizations	18
IV. Gaps and Way forward	18
V. Future Activities.....	20
3 - PROMOTING CYBER SECURITY	26
I. Background.....	26
II. Current activities.....	27
III. Co-operation with International Organizations	28
IV. Gaps and Ways to Address Them.....	29
V. The Way Forward	31
4 - ADDRESSING THREATS STEMMING FROM AFGHANISTAN	33
I. Background.....	33
II. Current activities.....	33
III. Co-operation with International Organizations	34
IV. Gaps and Ways to Address Them.....	34
V. Future activities.....	36
5 - PREVENTING THE PROLIFERATION OF WEAPONS OF MASS DESTRUCTION (WMD) IN THE CONTEXT OF UNSCR 1540	39
I. Background.....	39
II. Current Activities.....	40
III. Co-operation with International Organizations	40
IV. Gaps and Ways to Address them	41
V. Future Activities.....	41

PART 2: CONCLUSIONS AND RECOMMENDATIONS43

- Within the existing mandate of the Secretary General:44

- At the level of participating States:44

- Improving Co-operation with International Organizations:45

ANNEX 1 - A suggested list of possible decisions by participating States in thematic areas 47

INTRODUCTION:

This report is submitted by the Secretary General in accordance with MC.DEC/2/09 on Further OSCE Efforts to Address Transnational Threats and Challenges to Security and Stability with a view to strengthening the Organization's overall response, taking into account relevant mandates and the acquired experience of the OSCE executive structures. It attempts to propose some concrete steps that might be undertaken by the executive structures, and others that might merit further consideration by the participating States. These include both organizational measures aimed at strengthening systemic programmatic co-ordination among different executive structures tasked with addressing different aspects of transnational threats, as well as decisions that might be taken to close gaps in existing work, and to enable the OSCE executive structures to better assist the participating States to identify and address emerging transnational threats and challenges.

As noted in the Secretary General's first overview (SEC.GAL/64/10), OSCE activities aimed at addressing transnational threats have been geared toward specific threats, such as terrorism, organized crime and all kinds of trafficking, and specific capabilities, such as policing and border management. Experience has shown, however, that transnational threats, by definition, evolve rapidly, and that efforts to address them must be flexible and dynamic as well. A neat division between different aspects of transnational threats and OSCE responses, for example, between anti-terrorism and border management, or anti-trafficking and policing, are increasingly difficult. Effectiveness in addressing transnational threats requires not only a cross-dimensional perspective but also close co-ordination: among the Secretariat's Thematic Units, the Institutions and the field operations; between the OSCE and other international actors; and among the OSCE's participating States. The emergence of new challenges cutting across several of the OSCE's mandated areas of activity, such as trafficking in illicit drugs, organized crime, proliferation of WMD, and the diverse threats encountered in cyberspace, makes timely analysis of the threat, and effective co-ordination in addressing it, increasingly essential.

Intensified OSCE engagement with Afghanistan pursuant to MC.DEC/04/07 has placed additional pressure on the Organization to find effective approaches to inter-related transnational threats, and to ensure that the OSCE's efforts effectively complement other activities under way in the broader international community. The same is true for increased interest among participating States in finding ways in which the Organization can support the UN by further addressing the issues of WMD proliferation pursuant to UNSCR 1540. Each year, participating States augment the list of threats to be addressed by the OSCE.

The dynamism and growth of the OSCE's work to address transnational threats have presented many challenges for the Organization, particularly since increased demand has not always been accompanied by corresponding enhancement of mandates and increases in available resources. The need for an overall strategic perspective and enhanced stewardship at the political level has become more apparent. Current budgetary constraints might require the participating States to review existing priorities and mandates and consolidate activities with a view to focusing on those areas where the OSCE contribution – in terms of both resources and output – brings real added-value in relation to similar activities of other international actors. The 2003 OSCE Maastricht *Strategy to Address Threats to Security and Stability in the 21st Century* remains the main political basis on which participating States might enhance their efforts to combat both old and new threats. Yet the OSCE as a whole has not made the most of its inherent comparative advantages: its broad membership and geographic scope, its key role as a forum for political dialogue, its ability to serve as a hub of co-operation for officials, NGOs and international organizations, its network of Field Operations and its unique comprehensive and cooperative security mandate. While the Organization, over the past decade, has developed important expertise in individual areas related to transnational threats, its overall response has not lived up to the coherent vision set forth at Maastricht.

The extensive deliberation of the OSCE's role in combating transnational threats that has taken place in the framework of the Corfu Process has identified a broad common basis for enhanced efforts in this area, first of all due to the commonality of participating States' interests. The struggle against transnational threats is an area where the political will to find consensus is within reach. Progress in this area might become an engine for achieving results on other issues where participating States continue to hold divergent views.

The structure of the report is divided in two parts:

- **Part 1 - “Thematic Case Studies”** - highlights **five key areas of the OSCE work on transnational threats** – namely, *preventing and combating terrorism, fighting organized crime, promoting cyber security, addressing threats stemming from Afghanistan, and preventing proliferation of WMD in the context of UNSCR 1540*. These are the areas where the OSCE's ongoing and future activities cut across the mandates of various executive structures. Each chapter consists of a general description of the threat, a review of ongoing activities, identification of existing gaps and obstacles, and suggestions for addressing those gaps. The choice to focus on these particular areas is by no means a way to impose them on participating States as priorities for the Organization, or to substitute necessary political decisions by the decision-making bodies, but rather an attempt to present concrete cases as food-for thought for deliberations and subsequent decisions, if necessary.
- **Part 2 - “Conclusions and Recommendations”**, focuses on concrete steps that might be taken to enhance the effectiveness of the Organization's efforts to address the new generation of threats, and to fix the gaps identified in each thematic area, in order to strengthen programmatic coherence and synergy of effort among different structures. Some of these steps can be undertaken within the existing mandates of the executive structures, while others would require political decisions by the participating States.

Key Findings

A detailed examination of various forms of OSCE work aimed at addressing transnational threats leads to several general conclusions. Overall, current efforts could be strengthened through:

- Regular **review of the 2003 Maastricht Strategy**, with a view to updating the Organization's priorities in addressing transnational threats, and the relevant mandates of the executive structures.
- More systematic **co-ordination of various strands of "thematic" work** aimed at addressing transnational threats. This could be done in a number of ways, and several concrete options are put forward in the Conclusions and Recommendations section for the consideration of the participating States.
- More systematic **co-ordination of the work of Vienna-based thematic units with the related programme activity of the Institutions and field operations.**
- The **development of an analytical capacity within the Secretariat**, tasked with identifying emerging trends and the interrelationships between various forms of transnational threats.
- **Enhancement of the ability of the OSCE executive structures to deal with the evolving tools and methods applied by the perpetrators of transnational threats, particularly in cyberspace and counter-narcotics.**
- **More regularized co-operation with other international actors** in addressing transnational threats.

PART 1: THEMATIC CASE STUDIES

1 - PREVENTING AND COMBATING TERRORISM

I. Background

Globalization has greatly enhanced the ability to put subversive and criminal ideas into action through the growing ease of international travel, communication and transfer of money, combined with easier access to training and logistical support. Advances in technology have created the too real possibility of terrorist attacks using weapons of mass destruction (WMD). The Internet, in particular, has accelerated these trends and facilitated the radicalization and recruitment of disaffected young individuals into terrorist groups and networks.

These new conditions have significantly increased the efficacy of terrorism as an asymmetrical threat and made it an even more attractive tool for radical individuals and groups, offering them a global reach and the ability to inflict damage of catastrophic proportions.

Thus, for the foreseeable future, terrorism is likely to remain one of the most serious threats to the security and stability of OSCE participating States, and to the safety and well-being of our citizens.

Terrorism is a transnational and multi-dimensional threat. Terrorist ideologues invariably make use of existing social, ethnic and other grievances, and of distorted interpretations of widely accepted socio-philosophical or religious texts, to seek legitimacy and influence.

Also, terrorism is often closely linked to other organized criminal activities. Terrorists often use proceeds from criminal activities, such as drug trafficking or credit card fraud, to fund the commission of terrorist acts. They also use criminal networks to procure false identity and other documents to smuggle people, weapons and other materials across borders.

As terrorism is a transnational and multi-dimensional threat, the response to it must also be transnational and multi-dimensional. It should address the conditions that are conducive to the spread of terrorism and its ideological justifications, as well as terrorist activities themselves and their consequences.

The OSCE has sought to make a concrete contribution to such a response, reflecting both the nature of the threat and the Organization's comprehensive approach to security. The major OSCE documents that establish the political framework for the Organization's contribution to the global effort against terrorism, such as the Bucharest *Plan of Action for Combating Terrorism* (2001), the Porto *Charter on Preventing and Combating Terrorism* (2002), the Maastricht *Strategy to Address Threats to Security and Stability in the 21st Century* (2003), the Sofia *Ministerial Statement on Preventing and Combating Terrorism* (2004) and the Madrid *Ministerial Statement on Supporting the United Nations Global Counter-Terrorism Strategy* (2007) reflect this comprehensive approach.

In addition, over the years, the OSCE's decision-making bodies have adopted numerous decisions mandating concrete measures that the participating States should undertake in order to mitigate the terrorist threat, and capacity-building work to be undertaken by the OSCE executive structures.

II. Current Activities

In line with the aforementioned decisions and other documents, the OSCE executive structures have developed and are implementing a significant number of programmes in all three dimensions. These programmes focus on:

Addressing conditions conducive to the spread of terrorism, including ideological factors

The OSCE has sought to address long-term conditions that terrorists can exploit, while recognizing that none of these conditions can excuse or justify acts of terrorism. These conditions include protracted conflicts, dehumanization of potential victims, absence of the rule of law and violations of human rights, ethnic, national and religious discrimination and intolerance, political exclusion, socio-economic marginalization and the absence of good governance.

Recognizing the crucial importance of addressing the violent ideologies that underpin the terrorist threat, the OSCE participating States have sought to counter incitement to terrorism and the use of the Internet for terrorist purposes. These two phenomena are closely intertwined with, and constitute integral parts, of OSCE efforts aimed at addressing violent extremism and radicalization that lead to terrorism. Helsinki MC.DEC/10/08 called upon the participating States to make use of the OSCE executive structures in countering violent extremism and radicalization that lead to terrorism in their respective countries, encouraged participating States to continue to exchange ideas and national best practices in this field, and to enhance their co-operation with media, the business community, industry and civil society.

Strengthening the capabilities of participating States to mitigate the terrorist threat¹

The OSCE executive structures have put in place a number of capacity-building programmes areas aimed at enhancing the ability of the participating States to counter the terrorist threat. These include:

- **Strengthening the International Legal Framework against Terrorism, including the Ratification and Legislative Implementation of the Universal Anti-Terrorism Instruments (UATI);**
- **Enhancing international legal co-operation in criminal matters related to terrorism;**
- **Enhancing Travel Document Security (TDS), with four distinct sub-programmes:** (1) technological upgrades of travel documents, introduction of

¹ A comprehensive overview of OSCE counter-terrorism activities is contained in the **Report of the Secretary General on OSCE Counter-Terrorism Activities**, circulated to participating States on 1 April 2009 in implementation of MC.DEC/10/08

ePassports and promoting the ICAO Public Key Directory; (2) implementing the ICAO Minimum Security Standards for Handling and Issuance; (3) implementing border control solutions to allow for real-time access to INTERPOL databases, and (4) training border police on the detection of counterfeit travel documents;

- **Strengthening Public-Private Partnerships (PPPs) in Countering Terrorism** (especially in the areas of protecting vulnerable targets, preventing terrorist financing and engaging with the media);
- **Countering violent extremism and radicalization that lead to terrorism;**
- **Countering the use of the Internet for terrorist purposes/promoting a comprehensive approach to cyber security;**
- **Protecting non-nuclear critical energy infrastructure from terrorist attacks;**
- **Enhancing container/supply chain security;**
- **Addressing other current and emerging terrorist threats;**
- **Enhancing interaction with the OSCE Partners for Co-operation in the area of preventing and combating terrorism;**
- **Combating money laundering and terrorist financing;**
- **Strengthening transport security;**
- **Strengthening border security and management;**
- **Enhancing the overall capacities of police and law enforcement structures;**
- **Developing measures to prevent terrorists from gaining access to SALWs, other conventional weapons, weapons of mass destruction and related technologies including within the framework of UNSCR 1540; and**
- **Enhancing information exchange on counter terrorism developments through the Counter Terrorism Network.**

Protecting human rights, civil liberties and the rule of law in anti- terrorism actions

The OSCE and its participating States have repeatedly emphasized the central importance of respect for human rights in the struggle against terrorism. In 2002, an Anti-Terrorism Coordinator was established within ODIHR and the protection of human rights while countering terrorism was featured in discussions during that year's Human Dimension Implementation Meeting. With the creation of a Human Rights Department in 2003 and the elaboration of a full Human Rights and Anti-Terrorism Programme, ODIHR's work in this area has been instrumental in strengthening the will and capacity of participating States to respect human rights across the full range of efforts to combat terrorism, from prevention and disruption to investigation and prosecution.

In 2004, ODIHR collected and compiled anti-terrorism legislation from all OSCE participating States and made it available online. At the same time, ODIHR has emphasized that where national laws and procedures may differ, international human rights standards afford a common baseline for a shared response and international co-operation necessary to combat this transnational threat. ODIHR has also developed critical expertise and reference tools, in particular a manual on *Countering Terrorism, Protecting Human Rights*.

Since 2005, ODIHR has engaged in concrete capacity building activities, such as training for senior officials and practitioners on *Countering Terrorism, Protecting Human Rights*, and regular contributions to the delivery of technical assistance by other international and regional organizations, including the Council of Europe, the European Commission, the UN Office on Drugs and Crime and the UN Office of the High Commissioner for Human Rights.

Recognizing the value of sharing experiences and developing mechanisms for further co-operation, ODIHR has also focused on creating fora for the exchange of good practices and lessons learned on key topics such as solidarity with victims of terrorism (2006); human rights and international co-operation (2006); the role of civil society (2007); security, radicalization and the prevention of terrorism (2008); and understanding violent extremism and radicalization leading to terrorism (2009), cooperating with the ATU, OSCE field missions and other international organizations as appropriate.

III. Co-operation with International Organizations

The OSCE co-ordinates and co-operates extensively with other relevant organizations in the field of preventing and combating terrorism. High priority has been attached to work with organizations and bodies from the UN family, especially the UN Counter-Terrorism Committee (CTC) and its Executive Directorate (CTED), the 1267 and 1540 Committees, the Counter-Terrorism Implementation Task Force (CTITF), and the UN Office on Drugs and Crime (UNODC).

The UNODC turns to the OSCE for the organization of activities in promoting the international legal framework against terrorism and legal co-operation in criminal matters related to terrorism in the OSCE area. The UNCTC also routinely invites the OSCE to participate in its country assessment visits in the OSCE region. ICAO relies almost exclusively on the OSCE for the promotion and facilitation of global travel document security standards in the OSCE area, and has highlighted the support provided by the OSCE as a best practice to be followed by other regional organizations. INTERPOL considers the OSCE one of its main partners with regard to facilitating access to its databases. The UN 1267 Committee's Al-Qaida and Taliban Monitoring Team relies on OSCE support in promoting the UN anti-terrorism sanctions regime in the OSCE area. Similarly strong co-operation has been established with relevant international organizations, such as UNECE, OECD, WCO, IMO, ILO, IAEA and others, with regard to container/supply chain security, transport security, protection of non-nuclear critical energy infrastructure and other aspects of terrorism.

Co-operation with **relevant regional and sub-regional organizations** in the OSCE area is very important as well. Interaction between the OSCE and the **CoE** is especially strong due to the special relations between the two organizations and several joint activities have already been conducted over the years. Active has been the dialogue also with **EU, NATO, CIS,**

CSTO and **SCO**, which regularly participate in OSCE's activities and invite the OSCE to take part in their own activities, including counter-terrorism exercises.

Finally, in the framework of promoting and developing PPPs, the OSCE has established strong interaction with the private sector and civil society in many of these areas.

IV. Gaps and the Ways to Address Them

Gaps in the OSCE mandate:

The OSCE's work on preventing and combating terrorism provides an excellent example of how our organization is able to adapt to the evolving security threats and challenges and the concerns of its constituency. Nonetheless, the growth of the OSCE anti-terrorism agenda has also highlighted that new initiatives and tasks in the counter-terrorism area are often launched and pursued on an ad-hoc basis, without proper regard to their political or resource implications.

To a large extent, the **ATU** itself was established on an ad-hoc basis, more as an afterthought, rather than as a result of a serious deliberation. The Bucharest Plan of Action, which provides the most comprehensive strategic vision of the role of the OSCE in the fight against terrorism, had this to say with regard to what is now the ATU: it invited the Secretary General to consider "*the possible need for establishing an anti-terrorism unit or focal point within the Secretariat*".

As a result, the ATU does not have a strategically designed mandate that outlines its place in the OSCE family, its specific responsibilities or its ability to interface with other relevant international actors. The closest thing that exists to a mandate for the ATU is the following sentence in the Maastricht MC Decision on the Terms of Reference for the OSCE Counter-Terrorism Network (MC.DEC/6/03): "*Co-ordinate and facilitate OSCE counter-terrorism activities, including capacity-building assistance programmes, training and contingency-preparedness workshops, with a view to effectively utilizing resources and averting duplication.*" Evidently, only a very small part of what the ATU is expected to deliver today is reflected in this language.

The ongoing lack of a clear mandate is a significant obstacle to the ATU's efforts to function effectively as the OSCE focal point on all counter-terrorism issues and to ensure the coherence of the OSCE's anti-terrorism activities. Additionally, there are significant expectations of participating States for the analytical and conceptual services of the ATU and its interaction with research and academic institutions on the evolution of the terrorist threat and the responses to it.

Need for Resources:

The issue of resources is critical. The ATU has grown significantly since 2002. But its duties and tasks, the demands for its services and the expectations placed on it, have by far outpaced the growth in its personnel and its operating budget. As a result, the ATU finds itself at the limit of its ability to cope with its workload and is in danger of falling victim to its own success.

The Way Forward:

To address these gaps in mandate and resources, participating States are encouraged to consider the following:

- **Develop and adopt a comprehensive mandate** for the Action against Terrorism Unit, which would outline its main duties and responsibilities, as well as its place in the OSCE system. The ATU would serve as the focal point for all OSCE activities related to preventing and combating terrorism. It would provide analytical, conceptual and practical support to the CiO, Secretary General, participating States and all OSCE executive structures in the implementation of relevant commitments and tasks. It would maintain contacts with national authorities, relevant international bodies, experts and the private sector, in order to be able to develop and implement concrete projects to support national and international efforts. It would also support efforts in the UN context, especially with regard to the implementation of the Global Counter-Terrorism Strategy and relevant UN Security Council resolutions.

For the ATU to be able to effectively play the role of the OSCE counter-terrorism focal point, all executive structures should be encouraged to co-ordinate their own projects and activities with the Unit.

V. Future Activities

Based on MC and PC decisions adopted by participating States since 2001, the OSCE is expected to continue to pursue all of the programmes listed in Section II of this Chapter. However, taking into account the constant evolution of the terrorist threat and the security concerns of participating States, a number of additional areas for further strengthening of OSCE anti-terrorism work might be identified. Naturally, any future endeavours would be subject to the participating States' political and financial support.

Such areas might include:

- **Strengthening the security of mass transit transportation systems.** The OSCE – through both the ATU and OCEEA - has already conducted a number of activities with regard to transport security. Nonetheless, mass transit systems are inherently open and very difficult to control. Thus they remain a vulnerable and attractive target for terrorists. Building on already accumulated expertise and established networks, the OSCE could further enhance its input in strengthening national capacities to make such systems more secure.
- **Further strengthening the OSCE's contribution to the implementation of the UN Global Counter-Terrorism Strategy.** The OSCE is already doing a lot in this regard. However, as the Strategy represents a global blueprint for counter-terrorism action, the OSCE's work could be even stronger and more systematic, as outlined by the Madrid Ministerial Statement on Supporting the United Nations "Global Counter-Terrorism Strategy" (MC.DOC 3/07).

- **Strengthening the counter-terrorism role of victims/survivors of terrorist acts.** Once again, the OSCE has already done some work in this regard through the activities of ODIHR. However, until now this work has been focused on support and solidarity with the victims. It would be pertinent to consider how to strengthen the role that victims/survivors of terrorist acts and their families can play in the prevention of terrorism, especially in countering violent extremism and radicalization that lead to terrorism.
- **Strengthening identity management.** The improvement of the security features of travel and other identity documents has caused an increasingly prevalent global shift among criminals from document fraud to identity fraud and identity theft. In response, ICAO has launched a global initiative to improve national identity management. Given the severity of this “*identity threat*” and the fact that it affects virtually all of the OSCE participating States, and having in mind the existing OSCE acquis in travel document security, it would be natural for the OSCE to also become engaged in support of ICAO’s new initiative.
- **Strengthening PPPs in additional areas,** such as the tourism industry. Tourists and tourism infrastructure are preferred targets for terrorists, as they have broad public resonance and a significant economic impact. The OSCE can use its experience in promoting PPPs in other areas in order to strengthen interaction with the tourism industry and private security providers in enhancing the security of tourist sites and attractions.

I. Background

With the possible exception of the clan-type structures of criminal gangs in some regions of South Eastern Europe, contemporary organized crime does not generally conform to a hierarchal, familial structure. Instead it is characterized by opportunistic, entrepreneurial and fluid affiliations where syndicates form and dissolve for particular activities. There is also increasing evidence that ethnic or other characteristics like gender are becoming less of an inhibitor to criminal activity across networks or types of illicit activity. Strategic alliances forged between different groups aim at maximizing profit, and the opportunity for profit increasingly overrides the perceived safety provided by dealing with kin or known associates. Evidence from national investigations and prosecutions on human trafficking in OSCE participating States document the existing linkages between THB and drug trafficking, forging of documents, smuggling of migrants, and even terrorist activities.

Organized criminal networks have a detailed knowledge of law enforcement methodology, and take effective action to frustrate investigation of their activity. They are sophisticated, well-resourced and able to utilize the latest technology – including methods to abuse cyberspace for criminal purposes, the best in expert professional advice, and even the best legal defence in case the investigation reaches the courtroom. Furthermore, organized crime networks tend to display an ever-growing capacity to adapt their modus operandi to the law enforcement response, thus rapidly minimizing the effectiveness of repressive actions.

As a result of globalization and technological change, particularly in communications, criminal activity increasingly transcends physical and political boundaries. Organized crime investigations now commonly have a significant transnational component necessitating pursuit of targets, drugs, criminal assets and laundered money around the globe.

To respond to the threat of transnational organized crime, criminal justice agencies must be accountable, well trained and equipped with the technology that allows them to conduct professional investigations. International support could provide tailored assistance in the development of an effective criminal justice system that is free from corruption and inappropriate political interference, and assist law enforcement agencies with specialized training and the provision of technical resources. Moreover, international support could facilitate and enhance cross-border and international co-operation in defeating organized crime. However, international support can never substitute for local capacity and its ability to appreciate the ethnic, cultural and linguistic diversity.

Organized crime groups constitute a serious threat to the security of states and to the democratic functioning of societies. They generate large profits that are not only laundered and re-laundered in the legal economy but are also often used to bribe public officials and acquire political influence. Thus organized crime groups interfere with various aspects of society, politics and the economy, fuelling corruption, distorting free markets and undermining the rule of law and transparent decision-making processes.

The OSCE “acquis”

The OSCE participating States have adopted a number of Ministerial and Permanent Council Decisions relating to various aspects of the fight against organized crime, including combating trafficking in human beings and illicit drugs, the fight against money laundering and terrorist financing, the adoption of a Border Security and Management Concept, the enhancement of travel document security and decisions to encourage co-operation in the field of policing to combat organized crime and corruption. These decisions provide the basis for the OSCE approach to the fight against organized crime and the strengthening of criminal justice systems.

The OSCE’s “acquis” on combating organized crime has tasked the OSCE executive structures with building the capacities of criminal justice institutions, promoting the implementation of international conventions, and providing assistance to the participating States in translating relevant OSCE commitments and recommendations into reality. In the various consensus documents that the OSCE participating States have adopted in relation to the fight against organized crime, a number of international legal documents are mentioned and should be considered as part of the OSCE framework to address the fight against organized crime:

- The UN Convention against Transnational Organized Crime (Palermo Convention) and its supplementing protocols;
- The United Nations Convention against Corruption;
- The United Nations Anti-Drug Conventions of 1961, 1971 and 1988;
- Council of Europe Conventions and their protocols;
- Convention on the Transfer of Sentenced Persons (Strasbourg, 21 November 1983) and its 1997 Additional Protocol;
- Outcome of the Millennium Summit (2005 World Summit Outcome)
- The Financial Action Task Force’s (FATF) 40+9 recommendations to combat money laundering and terrorist financing.

II. Current Activities

Brussels MC.DEC/5/06 tasked the Secretary General to enhance co-ordination of OSCE activities in the field of organized crime. In response, the Secretary General created a Task Force on Organized Crime composed of representatives of the OSG, SPMU, OSR/CTHB, OCEEA, ATU, CPC, ODIHR and representatives of all OSCE field operations.

The Task Force has contributed to strengthening the capacity of the Organization to focus on organized crime by helping create informal networks of OSCE experts. It has also provided a formal structure whereby the cross-dimensional nature of OSCE efforts can be refined. It has encouraged more frequent contacts and channels of communication. The Strategic Police Matters Unit as a central contact point for organized crime issues has been tasked to facilitate co-operation and co-ordination across the OSCE.

The work of the Task Force is complemented by various programmes of thematic units and field operations designed to assist the participating States in improving and promoting the functioning of criminal justice systems, international legal co-operation, and implementation of international conventions.

OSCE efforts in relation to organized crime may be grouped into the following activities: *raising awareness, providing legal and institutional assistance, training and capacity building, facilitating co-operation/networking and providing equipment.* These activities are directed at various institutions and bodies that are involved in combating organized crime. The OSCE is assisting the participating States with a variety of approaches, such as:

- Preventive measures (e.g. travel document security; community policing as a crime prevention tool; measures to prevent all kinds of trafficking by educational and awareness raising efforts, measures aimed at addressing root causes, decreasing vulnerabilities to THB, assistance and protection to its victims (targeted also at preventing re-trafficking on THB), as well as working closely with media; border control and management);
- Supporting the enhancement of investigations, including forensics, financial investigations and tracking, seizure and confiscation of criminal assets;
- Promoting good governance to combat corruption and money laundering and financing terrorism through raising awareness of the international instruments in force and assisting participating States with the introduction of adequate legislation and compliance with international standards and commitments.

SPMU has developed a portal² on organized crime within its Policing OnLine Information System (POLIS). The portal facilitates access to reports, legislation, events, training materials, and a database of training centres offering training opportunities for foreign law enforcement.

The Office of Special Representative on Combating Trafficking in Human Beings (OSR/CTHB) has accomplished an exploratory study “Analyzing the Business Model of THB to Better Prevent the Crime” (under the UN.GIFT) aimed at helping decision-makers and practitioners in fine-tuning anti-trafficking policies and enhancing the efficiency of combating THB as a transnational (and national) threat. Other publications are also available on the OSR/CTHB web-page. The OSR/CTHB has also contributed to fostering bilateral and international co-operation on various aspects of anti-trafficking action including through promoting the establishment of and regular exchange among national co-ordination mechanisms.

The OS/Borders Team, through its capacity building, policy advice and cross border co-operation activities, supports participating States and their national border security and management agencies in addressing transnational organized crime. It reinforces the potential of these agencies to recognize and act against illegal cross-border activities.

The Office of the Co-ordinator of Economic and Environmental Activities (OCEEA) has been assisting the participating States in strengthening their capacity to adopt and implement international standards in combating corruption, money laundering and terrorist financing and, in some cases, to facilitate in the establishment of relevant institutions, in particular, financial intelligence units and anti-corruption agencies. Furthermore, the OSCE *Handbook on Best Practices in Combating Corruption* is used as a reference tool during training courses with legislators, government authorities, the business community and the civil society, as its best practice examples have proven useful for the drafting of legislation and the development

² <http://polis.osce.org/portals/orgcrime/>

of national strategies. The Handbook has been translated into six languages (English, Armenian, Azerbaijani, Macedonian, Russian, and Serbian).

Taking into account linkages between terrorism and organized crime and the increasingly similar tactics used by both, many of the programmatic activities of the ATU related to strengthening the participating States' capability to address the terrorist threat and implement their anti-terrorism commitments, such as enhancing travel document security and international legal co-operation, countering the use of Internet for terrorist purposes, enhancing container/supply chain security, and promoting public-private partnerships in countering terrorism also have relevance to preventing and countering organized crime.

III. Co-operation with International Organizations

The OSCE has developed a wide network of co-operation with institutions and regional and international organizations directly involved in activities to combat organized crime. It has developed a close relationship with UN agencies, in particular with the UNODC. The OSCE holds regular co-ordination meetings with the UNODC. Co-ordination meetings at the level of the Secretary General and the Director of UNODC have developed and boosted more productive and positive relations with the UNODC at the working level.

For instance, the SPMU holds a technical level round table meeting with the aim of agreeing on a joint work plan. The OSCE is the only non-UN family organization which participates in the Steering Committee (SC) of the UNODC-led United Nations Global Initiative to Fight Human Trafficking (UN.GIFT) and collaborates actively with the other members of the SC – UNODC, ILO, UNICEF, IOM, and UNHCHR.

The OSCE SR/CTHB has also established the *Alliance against Trafficking in Persons*, a unique informal platform for co-operation between the OSCE and other major international organizations and NGOs recognized for their active stand against modern slavery, one of the most serious forms of transnational organized crime.

As part of its efforts to strengthen relations with partner international organizations and bodies to combat money laundering, the OSCE was granted observer status at the Council of Europe's Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL). The main objective of the Committee is to evaluate the effectiveness of the national systems of member states to counter money laundering and financing of terrorism and to facilitate their compliance with the relevant international instruments. In addition, the OSCE obtained observer status in the Eurasian Group on Combating Money Laundering and the Financing of Terrorism (EAG) and has since then attended EAG Plenary Meetings. The OSCE has developed further co-operation with NATO, INTERPOL, Europol, CIS, CoE, CSTO, CARICC, SELEC, EAG and other platforms for exchanging experience, sharing good practices, and identifying emerging trends and priorities to meet transnational challenges.

IV. Gaps and Way forward

- The Task Force model, which has been successfully applied in the past in responding to PC.DEC/05/06, could be further improved by an internal mechanism that would obligate the OSCE executive structures to report to and co-ordinate their anti-

organized crime activities with a central point. Presently, information is shared on a voluntary basis. The Task Force could also facilitate programmatic synergy across the OSCE, and in particular could contribute to coherent programmatic objectives and outcomes.

- Participating States may wish to re-visit existing mandates in order to provide clearer and more coherent political guidance to the OSCE executive structures. Taking into account the fact that current mandates result from a series of ad hoc decisions taken in response to specific events, a comprehensive re-examining of those mandates might bring more clarity from the participating States as to what the OSCE should be doing in the area of combating organized crime, which may be reflected in the organizational structures of the OSCE.
- To further address the cross-dimensional aspects of transnational organized crime, the OSCE should further develop its research and analytical capabilities
- A separate Anti-Drug portal could be created in the Policing OnLine Information System. The portal would offer convenient access to various types of materials — reports and legislation, information on events and training opportunities for criminal justice agencies — all related to counter-narcotics.
- Building on its experience as facilitator of international co-operation, the OSCE should lead new initiatives to support and catalyze the development of specific bilateral or multilateral agreements – as appropriate – to facilitate international law-enforcement co-operation on combating organized crime. To this end, the OSCE Secretariat could be mandated to initiate a consultation with the General Prosecutors of participating States and launch an initiative to support the establishment of Prosecutors Network.
- The OSR/CTHB could further develop its capacity building activities and develop multi-disciplinary curricula for specialized law enforcement and prosecutorial authorities on trafficking in human beings, as well as for lawyers specialized in legal counselling and assistance to victims of the crime. At the same time, the OSR/CTHB should promote the networking of law enforcement and prosecutorial authorities, with a view to facilitating the involvement of specialized units, including financial units, in international law enforcement and judicial co-operation.
- The OSCE will facilitate the dialogue on the linkages between money laundering and drug trafficking and trafficking in human beings, thus being proactive in an area which in the auspices of the international community is not yet sufficiently developed.
- Building on its experience in facilitating interagency and international co-operation, the OSCE will further develop dialogue and training for criminal justice and law enforcement authorities on the legal requirements, procedures and available tools for the identification, confiscation and recovery of assets deriving from criminal activities.
- Effective outreach and co-operation with the Partners for Co-operation, in particular with Afghanistan, where many transnational threats converge, will be essential to the OSCE's success. The OSCE has already implemented a number of successful training

courses for the Afghan Law Enforcement Officials in the Russian Federation and Tajikistan, and will continue this effort.

- In responding to organized crime issues, more emphasis to be placed on crime prevention measures, which should be enhanced in the framework of the police-public partnerships (community policing) programmes. The OSCE's unique cross-dimensional approach, its widespread field presence, especially in regions experiencing problems with types of organized crime such as drug trafficking, and its broad acceptance by civil society place the Organization in a strong position to mobilize an inter-agency response to address these issues. The Organization, in close co-ordination with the UNODC and other interested international/regional organizations should therefore continue to identify new ways to further enhance regional co-operation and build capacity in law enforcement agencies in order to enable them to respond more effectively to drug trafficking and trafficking in human beings.

V. Future Activities

Organized crime is facilitated by corruption, and this challenge must be tackled in any attempt to provide a meaningful response. There is a raft of legislation available to address corruption, but this legislation is often ignored. The various facets of organized crime are closely linked where syndicates form and dissolve to pursue particular activities, driven by demand and opportunity.

Because of this fluidity, responses to organized crime must take account of a broad range of activities and just focus on one manifestation of the problem. There is significant evidence that drug traffickers use the same routes, modus operandi, and service providers to traffic human beings and small arms. Financial gain is the common denominator, and this needs to be recognized and addressed as part of the overall response. International legislation that relates to transnational investigations of money laundering as well as to asset confiscation and forfeiture needs to be reflected and pursued in national legislation, as well as the right of trafficked persons to compensation for the harm suffered.

OSCE experience shows that there is a continuing need to focus on identifying gaps in the legal framework of participating States and encouraging them to commit to and implement the major international treaties and conventions in the field of the fight against organized crime, specifically the UNTOC and international conventions on combating illicit drugs.

Programmatic priority areas in combating organized crime are elaborated in following paragraphs.

Combating Trafficking in Human Beings

THB remains a widespread phenomenon throughout the OSCE area with a minimum estimate of 2.45 million victims of trafficking globally, out of which at least half a million are in the

OSCE area.³ Criminal profits derived from Trafficking in Human Beings are estimated at about USD 32 billion globally.⁴

Investigations carried out at the national level have confirmed that THB may involve different types of organized crime, ranging from highly structured international trafficking networks to loosely connected clusters of people, together forming a very flexible and specialized trafficking network that is difficult to disrupt.⁵ Furthermore, as mentioned above, linkages exist between THB and drug trafficking, corruption, money laundering, forging of documents, fraud, smuggling of migrants, and terrorist activities.

At the same time, reported criminal proceedings for trafficking in human beings are relatively modest. It is reasonable to assume that many criminal proceedings are carried out on the basis of indictments for less serious crimes. This implies that the criminal justice response is not comparable with the scale of the crime; moreover, only final exploiters are targeted, mainly in the field of sexual exploitation; the level of penalties is low compared to the gravity of the crime; no seizure or confiscation of the proceeds of crime is carried out in the vast majority of cases.

Therefore, THB is still low-risk compared to other types of organized crime. Anti-trafficking action in the field of prosecution should aim at increasing the impact and the deterrent effect of the criminal justice response. This means that the response should meet the new challenges deriving from: the massive scale of the crime, the growing (and often prevailing) trend of THB for labour exploitation, and the increasing reinvestment of the proceeds of crime and money laundering.

For this purpose, a common strategic goal of OSCE participating States is to raise the profile and quality of investigations in THB cases, while pursuing human rights based approach in the implementation of all anti-trafficking measures which has proven its highest efficiency for the successful prosecution.

Therefore, the operationalization of this goal could include analysis and research including on the implementation of codes of conduct and other measures, such as:

- increasing the capacity of law enforcement operational units, especially those specialised or in charge of THB cases and/or organized crime cases;
- generalizing the use of the most advanced and sophisticated investigative tools such as phone tapping, electronic surveillance, financial investigation and under-cover operations;
- promoting the full involvement and co-operation of specialized financial police units, to trace financial operations linked with THB cases, and ensure confiscation of the proceeds;
- promoting capacity building of practitioners, particularly aimed at giving legal counselling and assistance to trafficked persons, and help them to claim pay-back of wages and compensation;

³ ILO, A global alliance against forced labour, Geneva 2005.

⁴ Ibid.

⁵ Analysing the Business Model of Trafficking in Human Beings to Better Prevent the Crime. OSCE-UN.GIFT Report, 2010

- promoting the international networking of police and prosecutorial specialized units, with a view to facilitating international law enforcement and judicial co-operation, including the use of joint investigation teams.

The OSCE is unique as an organization in that it takes a comprehensive approach to combating THB across all the three dimensions of security. The OSCE is well placed to engage with and assist participating States in the implementation and advancement of anti-trafficking efforts, through its Office of the Special Representative and Co-ordinator for Combating THB, the ODIHR anti-Trafficking Programme and the Focal Points in field operations, as well as other OSCE structures, working in close co-operation with the *Alliance against Trafficking in Persons* partner international organizations and NGOs.

The OSR/CTHB has been considerably raising awareness among the participating States through the *Alliance against Trafficking in Persons* high-level conferences and technical seminars, its numerous publications on the most challenging THB issues and through its website. It contributed to the capacity building for the law enforcement and the judiciary, as well as migration officers and the military, through providing regular training at the International Training Centre on Migration and CTHB in Minsk, at the NATO Partnership-for-Peace Training Centre in Ankara, and, organized by field operations, in the host countries upon request, such as the recent joint training on challenges of investigating THB for police and prosecutors at the Uzbek Ministry of Interior.

The OSCE SR/CTHB, as well as the ODIHR and field operations are engaged in constructive dialogue with the OSCE participating States, aimed at providing assistance in the areas of legislation, assessment of the effectiveness of current responses and identification of best practices, promotion of national coordinating structures and national monitoring and reporting mechanisms, National Action Plans and Programmes. All these activities are designed to help in the implementation of the OSCE anti-trafficking commitments and international obligations related to combating THB as a serious transnational threat affecting both individuals and States.

Combating Drug Trafficking

The OSCE's most valuable contribution to international co-operation would be to focus on supporting co-ordination mechanisms. Strengthening co-ordination and co-operation with the INCB, UNODC, Paris Pact, CSTO, CARICC, SELEC and other relevant international and regional structures are essential because resources are meagre; furthermore, they are also needed to ensure coherent approaches. This implies dividing labour, sharing costs and avoiding unnecessary duplications among international players and bilateral donors. Reinforcing the established patterns of co-operation and further creating re-invigorated innovative approaches for co-ordination are needed.

All OSCE participating States have signed and ratified three international anti-narcotics conventions, namely; the "Single Convention on Narcotic Drugs (1961), Convention on Psychotropic Substances (1971), Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (1988). Further efforts of participating States and enhanced support from the OSCE executive structures are needed in order to make full use of these Conventions, inter alia, through mutual legal assistance and extradition of drug criminals, as envisioned by the PC.DEC.813.

Working closely with other relevant international and regional organizations, the OSCE could provide assistance in developing an effective and comprehensive international approach to illicit trafficking in narcotic drugs throughout the OSCE area. This assistance may focus on promoting dialogue, information sharing and best practices among national anti-drug services and other competent national structures, promoting cross-border co-operation aimed at countering illicit traffic in narcotic drugs and chemical precursors, supporting improvement of national strategies and action plans, developing projects on enhancement of law enforcement agencies' capacities in combating production and trafficking in drugs and in strengthening control of precursors, as well as conducting training programmes.

The OSCE's executive structures, their programmatic activities and networks with participating States and key international actors present opportunities for the Organization to engage in public outreach activities that could assist in drug supply reduction and illicit drug abuse prevention.

The OSCE has organized a number of regional workshops and OSCE-wide conferences that have addressed various aspects of illicit drug trafficking, enhancement of law enforcement co-operation in drug supply reduction, control of precursors, and good practices on operational issues. These events contributed to more productive regional co-operation among various law enforcement agencies on prevention, identification, detection and investigation of drug-related crimes, mutual legal assistance, extradition and criminal assets recovery, as well as in the area of controlled deliveries of illicit drugs. The Organization will continue to organize similar events to support co-operation and the exchange of good practices among the participating States.

Police and public partnerships are a useful tool, both to prevent abuse and to combat the selling of illegal drugs. In this respect, good practices will be identified, promoted and shared with the participating States.

Co-operation and information exchange at the regional level between and among the offices of international organizations and local regional mechanisms, as well as the competent authorities of participating States will be further improved by utilizing the existing OSCE tools such as the Policing OnLine information System (POLIS) and Border Security and Management National Focal Point Network, as well as by developing guidebooks and manuals and promoting public-private partnerships in addressing the drug problem.

In order to enable comprehensive actions by the OSCE participating States and the OSCE executive structures in combating the threat of illicit drugs and diversion of precursors a possibility of elaborating an OSCE strategic document/action plan on counter-narcotics efforts, as well as enhancing anti-drugs capacities within the OSCE Secretariat could be considered.

Terrorism and Organized Crime

While not always evident, there are links and similarities between organized crime and terrorism, which make it possible to mitigate both threats with the same measures. For instance, terrorists often use proceeds from criminal activities, such as drug trafficking or credit card fraud, to fund the commission of terrorist acts. They also use criminal networks to procure false identity and other documents, to smuggle people and materials across borders.

With this in view, some of OSCE's anti-terrorism programmes have relevance also with regard to the fight against organized crime.

The ATU travel document security programme is one of the OSCE's longest running anti-terrorism programmes. As criminals also rely on fake or fraudulent travel documents, by definition everything that the national authorities do to strengthen travel document security from an anti-terrorism perspective has a direct and positive impact also in combating/preventing organized crime.

Enhancing container/supply chain security is also directly relevant to preventing/combating organized crime. Ensuring greater control over containers, standardization of accompanying documents, advanced information submission and the ability to track the movements and handling of containers from their point of origin to their final destination will serve to prevent the use of containers not only for terrorist purposes, but also for other criminal activities, especially for the trafficking in drugs, weapons and human beings and the smuggling of goods.

Police-Related Activities in Combating Organized Crime

The UN Convention against Transnational Organized Crime (UNTOC), together with its Protocols, is the primary international legal instrument in the fight against organized crime. Forty-nine OSCE participating States have ratified the Convention and an additional six have signed it and are waiting for ratification. Significant work remains, however, in bringing the Convention to life by fully implementing its Articles and Protocols. SPMU has already engaged in significant work, in co-operation with the UNODC, by organizing a variety of conferences and training seminars that have provided legal training for practitioners and raised awareness among the OSCE delegations.

SPMU will continue to assist participating States in the full implementation of the UNTOC and its Protocols. Due to SPMU's mandate to provide law enforcement training, it will direct its efforts toward building law enforcement capacity. Particular attention will be focused on the Articles of the UNTOC related to the confiscation of the proceeds of crime, mutual legal assistance, joint investigations, special investigative techniques, exchange of information and law enforcement co-operation. These areas are critical aspects in combating organized crime. The identification and confiscation of criminal assets is one of the most effective methods in dismantling organized crime networks. In order to be effective, law enforcement agencies must possess the technical skills to carry out these responsibilities. This is especially true when dealing with requests for assistance by foreign law enforcement agencies. A law enforcement agency that has initiated an organized crime investigation must be able to rely on the competency of other agencies when investigations cross borders. Investigations will also be more successful if formal and informal networks are established in order to process requests more efficiently. SPMU will promote and support activities to assist participating States in achieving the necessary level of skill to enrol in existing international criminal investigation networks.

The UNTOC defines an organized criminal group as two or more persons committing a serious crime for financial benefit. A significant number of cyber crimes fall within this definition, especially online fraud and the distribution of child pornography. The SPMU will continue its training activities to assist participating States in acquiring the technical skills they need to prevent and investigate organized crime activities conducted via the Internet. It

will also promote the development of specialized cyber crime capacities to handle international requests for assistance. Computer forensics and the proper management of electronic evidence is also an important factor in achieving successful outcomes in international organized crime investigations. Such activities can involve everything from tracking mobile telephone calls to extracting information from computer hard drives.

Tackling Corruption, Money Laundering and Terrorist Financing

Weak governance, absence of the rule of law and the lack of transparency and accountability provide a fertile environment for corruption, money laundering and financing of terrorism, all of which are closely connected to organized crime. Criminal groups operate better where there is less public accountability of government institutions, generally inadequate legislative regimes and law enforcement activity or a lack of specialized personnel to fight their advanced criminal methods.

Tackling organized crime and its linkages with money laundering and terrorist financing has become even more urgent under current circumstances, where the global financial and economic crisis has affected every country irrespectively of the level of development. For example, as already evidenced by the international community, networks active in various types of organized crime take advantage of weak national structures in order to penetrate financial markets and launder large amounts of money by channelling it to institutions striving to survive the credit crisis.

However, the implementation of adopted legislative frameworks is also essential in fighting organized crime and therefore the OSCE will pay particular attention to capacity building and training activities in co-operation with partner Organizations. For example, the investigative capacity of law enforcement authorities should be improved; the lack of specialization of the prosecution and judiciary on economic crime issues should be tackled, and the capacity of staff of financial intelligence units strengthened, *inter alia*, on reporting suspicious transactions in relation to money laundering and terrorist financing.

More attention will also be afforded by the OSCE to involving civil society. National systems should provide the necessary mechanisms for citizens to be involved in legal reforms, and to assist in dealing with corruption complaints.

I. Background

Growing dependence on information technology (IT) and the interconnection of critical infrastructure have made a secure cyberspace vital to the functioning of a modern state. At the same time, advances in the IT sector have also presented terrorists and other criminals with new opportunities and attack vectors, which they are increasingly exploiting. Perpetrators of cyber crimes share common methods, even if their goals and motivations differ. They learn from each other and frequently work together. Moreover, the risk of traditional inter-State conflicts extending into cyber space is growing.

The OSCE participating States have recognized that the Internet has also become a key instrument for transnational illegal activities – a threat that targets governments, public and private institutions, the private sector and individuals and that uses the Internet (a) to perpetrate profit-oriented cyber crimes; (b) to support terrorist activities; and (c) to support other organized criminal activities, including trafficking in human beings.⁶ Perpetrators of terrorism, organized crime, various forms of trafficking and other transnational threats the OSCE is already mandated to address are increasingly moving into cyberspace – in order to remain effective in its overall response to these threats, the OSCE needs to do the same.

In fact, the Internet has become both a delivery system and a logistical support system for a wide spectrum of criminal and terrorist activities. Given the diverse and cross-cutting nature of the threat, a number of OSCE structures (ATU, SPMU, FSC SU, OCEEA, OSR/CTHB, RFoM, ODIHR and several Field Operations) are involved in activities related to cyber security, making effective co-ordination of efforts essential to their success.

Concerned over the extent of the use of the Internet by terrorist organizations, the participating States adopted MC.DEC/3/04 and MC.DEC/7/06. These were the first official OSCE documents dealing with threats emanating from cyberspace, and serve as the basis for the ATU's ongoing active role in this area. Specifically, the participating States committed to exchange information on the use of the Internet for terrorist purposes and to identify possible strategies to combat this threat, while ensuring respect for relevant international human rights obligations and standards (MC.DEC/3/04). They further decided to intensify their action by enhancing international co-operation on countering the use of the Internet for terrorist purposes; to consider taking all appropriate measures to protect vital critical information infrastructures and networks against the threat of cyber attacks; to consider becoming party to and to implement their obligations under the existing international and regional legal instruments; and to explore the possibility of more active engagement of civil society institutions and the private sector in preventing and countering the use of the Internet for terrorist purposes (MC.DEC/7/06).

⁶ The increasing use of the Internet by criminals to traffic human beings endangers individuals seeking employment and other ways to change or improve their lives through educational opportunities, marriage (e.g. mail order brides, etc.). According to law enforcement, the recruitment of potential victims of human trafficking commonly takes place through fake and deceptive advertising, announcements and invitations placed on the web. This is also the means used for money laundering of the huge profits from THB, to transfer payments for child online pornography. The Internet is also a major way for traffickers and online exploiters to lure children, to "normalize" online child exploitation, and to facilitate child sex tourism. Approaches to fight these ever changing tactics are to work to enhance child protection, and expand criminal liability, and territorial jurisdiction to prosecute online exploitation and trafficking of all forms through the internet.

In addition, building on MC.DEC/10/08 and in particular MC.DEC/5/07 on promoting public-private partnerships in combating terrorism, the Organization has involved the private sector, civil society and academia in its cyber security activities as appropriate.⁷

Many participating States have expressed support for a more comprehensive approach to cyber security, as reflected in FSC.DEC/10/08 in which participating States decided to organize an OSCE Workshop on a *Comprehensive OSCE Approach to Enhancing Cyber Security* (17-18 March 2009, Vienna) with the participation of relevant international organizations.

Furthermore, MC.DEC/9/07 on *Combating Sexual Exploitation of Children on the Internet* focused specifically on one particular use of the Internet by criminal networks.

II. Current activities

To date, the OSCE has been engaged to a limited extent in addressing individual aspects of cyber security, such as combating cybercrime and combating the use of the Internet for terrorist purposes – all the while ensuring that efforts to enhance cyber security do not impinge upon fundamental freedoms such as freedom of expression and assembly on the Internet. Over the years, however, pertinent OSCE activities have evolved in line with the threat. As a result, recent events organized by the OSCE – and in particular those organized/facilitated by the ATU and the SMPU in 2009 – have promoted a more comprehensive approach to cyber security.

Such an approach is based on the understanding that the widespread use of the Internet by terrorists, traffickers and criminals make it increasingly difficult to develop effective responses to transnational threats without promoting a more secure cyberspace. A comprehensive approach to cyber security should: (a) strengthen national security; (b) tackle cybercrime; (c) inhibit terrorist use of the Internet; (d) be responsive to a wide variety of risks and threats, including politico-military; and (e) enable competent authorities to protect a wide spectrum of targets ranging from the individual Internet user to critical infrastructures; and (f) safeguard the Internet as a space for free expression and assembly.

An OSCE-wide workshop in March 2009 not only enhanced awareness of possible steps to comprehensively strengthen cyber security. It also resulted in recommendations and suggestions on the future role of the OSCE in this thematic area (FSC.DEL/92/09), which remain under consideration by the participating States. Similarly, two national expert workshops organized by the ATU in 2009, in Serbia and in Croatia, resulted in recommendations for national decision makers. Moreover, as a follow-up to the Serbia workshop (February 2009, Belgrade) and the 2008 OSCE Police Experts Meeting, the SPMU and McAfee Labs organized a training workshop for law enforcement officers on dealing with cyber threats (December 2009, also in Belgrade).

⁷ Public-Private Partnerships (PPP) are a key contributor to enhanced cyber security – not only because the private sector researches, designs, develops, builds and maintains many of the most commonly used information technologies – but also because industry owns many of the world's critical infrastructures and usually operates them with the main goal of turning a profit rather than being as secure as possible. Moreover, academia has an important role to play in terms of conducting research on combating cyber threats while civil society can offer vital contributions to countering the terrorist message on the Internet.

III. Co-operation with International Organizations

A number of other international and regional organizations are working on certain cyber security topics.

Several **United Nations** entities, including the Counter Terrorism Implementation Task Force (CTITF), the Office on Drugs and Crime (UNODC), the International Telecommunications Union (ITU), the General Assembly (UNGA), and the Internet Governance Forum (IGF), are actively dealing with various aspects of cyber security, such as awareness raising, combating cybercrime, and combating terrorist use of the Internet at the global level.

The **Council of Europe (CoE)** has been particularly active in combating cybercrime, with a special focus on developing a legal framework. The CoE's Convention on Cybercrime (2001) is currently the only legally binding international instrument in this area, and the CoE also helps countries to accede to, ratify and implement the Convention through technical co-operation projects.

A number of **European Union (EU)** bodies have also been active in various areas of cyber security. These include European Network and Information Security Agency (ENISA) and the European Commission, both dealing with issues such as capacity building, combating cybercrime as well as terrorist use of the Internet, and enhancing critical infrastructure protection.

The **North Atlantic Treaty Organization (NATO)** has been working since 2002 on technical aspects of cyber security. A NATO cyber defence policy was approved in 2008 and is currently being implemented. Although the exact details of the NATO Policy on Cyber Defence remain classified, the establishment of the Co-operative Cyber Defence Centre of Excellence (CCD CoE) is a noteworthy step taken in line with it.

The **Commonwealth of Independent States (CIS)** and the **Shanghai Co-operation Organization (SCO)** have also addressed cyber security in their work. The CIS participating States have signed an Agreement on Co-operation in the Fight against Cybercrime and the SCO has adopted a political Declaration on Information Security and a follow-up Action Plan; the SCO Member States signed an Agreement on Co-operation in the Field of International Information Security. These documents seek to address such issues as information exchange, co-operation in investigation and training, as well as the development of relevant legislation.

Co-operation with international and regional entities also active in this thematic area has, from the outset, been a hallmark of pertinent OSCE efforts. Strong working-level partnerships have been established with the **UN** (terrorist use of the Internet; combating trafficking in human beings and money laundering), **CoE** (cybercrime), **NATO** (terrorist use of the Internet; critical infrastructure protection), **EU** (critical infrastructure protection) and **OAS** (terrorist use of the Internet; cybercrime), **EUROPOL** (Investigative Techniques for Law Enforcement), **ICMEC** (Sexual Exploitation of Children on the Internet) – illustrated by frequent direct involvement of these bodies in relevant OSCE activities and vice versa (e.g. workshops, trainings, conferences, consultations).

The OSCE should seek to also establish co-operation mechanisms with new partners, in particular with entities such as the CSTO and SCO, and to explore co-operation with bodies active outside the OSCE region such as APEC, ASEAN and the Organization of American States (OAS).

IV. Gaps and Ways to Address Them

External:

As mentioned above, a number of international and regional organizations are working on various cyber security topics. On the whole, however, their work has traditionally focused on only one or a few aspects of cyber security rather than attempting to tackle the issue comprehensively. To put the OSCE's efforts to promote a comprehensive approach to cyber security into context, we have to consider the following challenges currently faced by cyber security practitioners:

- The international community lacks a shared and common response to cyber security threats. All too often it is divided in the use of resources, expertise, approaches, functional jurisdictions and legal frameworks. Many countries have not reviewed or updated their national legislation to deal effectively with cyber threats. Similarly, many do not seem to have developed national strategies that deal specifically with enhancing cyber security. Moreover, many countries have still not established specialized Computer Emergency Response Teams (CERTs) or Computer Security Incident Response Teams (CSIRTs) tasked with tackling the latest cyber security challenges. On the whole, research is lacking about the extent to which countries are dependent on their critical cyber infrastructure. Similarly, research is lacking on how vulnerable critical infrastructure generally is to cyber attack and on how to reliably trace the origin of cyber attacks. In addition, public-private-partnerships (PPP) with industry and academia are not sought or utilized in a systematic manner, even though industry expertise and academic research could bring large benefits during the drafting of national cyber security strategies and during the elaboration of new legislation aimed at tackling cyber threats. Importantly, end-user education is not systematically promoted in the OSCE region and beyond – even though non-security conscious IT users represent arguably the most problematic “enabler” of some of the most dangerous types of cyber attack.⁸
- Importantly, end-user education should take into account gender differences in the use of the Internet.⁹ Since many countries are promoting the access and use of the Internet as a fundamental freedom and also promote entrepreneurship through the use of Internet based technologies, the impact of the Internet and the potential exposure of specific groups of Internet-users (men, women, boys and girls) to acts of cybercrime are likely to increase. End-user education, focusing on awareness raising and capacity building, and corresponding to gender differences in the use of Internet and exposure to specific risks will become more important.

⁸ E.g. large-scale (Distributed) Denial-of-Service attacks, in particular those relying on Botnets.

⁹ While existing research reveals that gender-differences in the use of the Internet by men and women in terms of overall usage are decreasing, there are indications that women use the Internet for interpersonal communication, information search, or education, whereas men use the Internet for one-way communication entertainment, or trade/personal finance. Furthermore, the use of the Internet changes according to gender, age, and education level, exposing women, men, girls and boys differently to cyber-crime and to terrorist activities on the internet. See S. Banerjee, H. Kang, S. Bagchi-Sen, H.R. Rao, “Gender Divide in the use of Internet Applications”, published in the International Journal of E-Business Research, April-June Issue, 2005, page 24-39.

- Moreover, the Internet has a tremendous potential in crime prevention – a potential that has, thus far, not been adequately explored by the international community.¹⁰

Internal:

- Intra-organizational co-operation has been ongoing and effective, albeit on an ad-hoc basis and often dependent on personal relationships. It includes partnerships such as those among the ATU-SPMU-OCEEA – during the *National Expert Workshop on Combating Terrorist Use of the Internet and Comprehensively Enhancing Cybersecurity* (February 2009) where SPMU and OCEEA participated in the form of moderator and expert presenter respectively – and the SPMU-OSR/CTHB – during the *Online Conference on Sexual Exploitation of Children on the Internet* (October 2008).
- As more OSCE structures become involved in activities to enhance cyber security, the executive structures have made efforts to establish more structured, systematic and efficient co-operation mechanisms (e.g. Task Forces or Working Groups, staff level meetings) and to agree on clear divisions of labor. Generally, the ATU has focused on issues pertaining to *prevention* while the SPMU has focused on issues pertaining to law enforcement capacity building on *investigation* of cyber incidents. The contributions of OSCE institutions to efforts to enhance Organization-wide co-ordination could be significantly improved.
- Clearly, the number of tasks related to enhancing cyber security by participating States has increased substantially over the last two years. More and more participating States fully realize the national security implications of securing cyberspace – as evidenced by discussions in the framework of the Corfu Process. Moreover, other threats the OSCE is already mandated to address, such as terrorism, trafficking and organized crime, are increasingly present in cyberspace. In addition, as mentioned previously, the risk of traditional inter-state conflicts extending into cyberspace is increasing, which is likely to require an OSCE response. Further increasing the workload of the existing structures and OSCE staff without enhancing the Organization's ability to address cyber threats more comprehensively could lead to a reduction of the quality and effectiveness of existing programmatic efforts.
- More importantly, the establishment of a clear and strong mandate on cyber security would substantially strengthen the OSCE's ability to develop effective responses to cyber threats. Current OSCE mandates have established the OSCE as an authority on various aspects of enhancing cyber security. Work to date, however, has treated cyber threats as peripheral aspects of work in other areas (terrorism, trafficking, organized crime, etc.). A more comprehensive approach that enabled the Organization to develop the necessary tools and expertise to deal effectively with threats in cyberspace would strengthen its efforts in addressing transnational threats more generally.

¹⁰ It could, e.g. be further explored how to best prevent, block or intercept online recruitment, exploitation and abuse, how to counter disinformation spread with criminal intent, how to use the Internet to investigate the use of the Internet in trafficking in human beings, how to track money laundering and how to find criminal assets online.

V. The Way Forward

The OSCE has been a pioneer in promoting a comprehensive approach to security, and it has a proven track record of successful initiatives pertaining to a number of threats to cyber security, including cybercrime, trafficking in human beings, terrorist use of the Internet and threats to critical infrastructures. In addition, the OSCE is well positioned to address all these issues with the necessary regard for human rights and civil liberties. Thematic Units have already established extensive networks of top-class cyber security experts from the public and the private sectors – and also from other international and regional organizations – who are keen on working with the OSCE on this issue.

Clearly, the individual work of national authorities, international and regional entities, and other structures, has contributed to e.g. countering cybercrime and terrorist use of the Internet. However, on the whole it has traditionally focused on only one or a few aspects of cyber security rather than tackle the issue comprehensively. The OSCE role would be the following:

- To **comprehensively enhance cyber security** in the OSCE region by providing participating States with concrete options for responses to national and regional cyber security challenges;
- To **support global cyber security** efforts led by the **United Nations** and further strengthen co-operation with other regional actors active in this thematic area;
- To **enhance the effectiveness of the OSCE's existing efforts** to address transnational threats, by developing the requisite expert networks to develop effective responses to cyber threats.

In order to achieve the above aims, it may be necessary to **strengthen the OSCE's mandate** for comprehensively enhancing cyber security and to **streamline/re-structure the OSCE's organizational layout** in such a manner that the above two aims can best be achieved.

In light of the present interest in comprehensively enhancing cyber security and the OSCE's momentum in this thematic area, an elaboration of an *OSCE [Strategy/Concept / Framework/ Guidelines] on Comprehensively Enhancing Cyber Security*. Such a document could enable participating States to harmonize their cyber security priorities and approaches by outlining certain common principles of state behaviour in the sphere of cyber security. It could also seek to identify the most dangerous threats to cyber security from state and non-state actors, and the primary sources of these threats. It could tie together the OSCE's existing efforts to address various strands of cyber security, establishing a clearly identifiable cyber security focal point to support the efforts of programmes in the Secretariat, the Institutions and the field operations, while offering expert advice to the participating States on how to address cyber threats in a comprehensive and co-operative manner.

Importantly, the document could also take into account previous work done by other regional and international actors. In particular, it could strongly support global cyber security efforts led by the United Nations with a focus on adding value by utilising the unique strengths of the OSCE. It would be advisable, if this document would be complemented with the establishment of a mechanism to assist participating States in its implementation, which might include proposals to streamline/re-structure the Secretariat's organizational layout.

To respond to the increased demand for OSCE cyber security engagement and in order to assist in the implementation of an OSCE document on comprehensively enhancing cyber security, participating States might consider the creation of a new OSCE structure as a focal point for cyber security threats and challenges – **a Cyber Security Unit (CSU) in the Secretariat.**

Such a structure would build on past OSCE efforts to address various aspects of cyber security serving as the focal point for all OSCE activities related to comprehensively enhancing cyber security. It would provide analytical, conceptual and practical support to the CiO, the Secretary General, the participating States and all OSCE executive structures. The Unit would also maintain contacts with national authorities, relevant international bodies, experts and the private sector, in order to identify and analyse new developments, threats and challenges in cyber space, propose policy options and practical recommendations on how to address them within the OSCE framework and develop and implement concrete projects to support national and international efforts in that regard. It would also support efforts in the UN context to address cyber threats.

A potential new Cyber Security Unit could further expand the Organization’s contributions in this area by:

- **Enhancing awareness-raising activities.** These events would build on previous OSCE activities and promote a comprehensive approach to cyber security. Individual sessions could focus on (a) possible norms for State-to-State behavior in cyber space; (b) combating cybercrime; (c) combating terrorist use of the Internet and cyber attacks by terrorist groups; (d) protecting critical infrastructure from cyber attacks; (e) promoting pertinent public-private-partnerships; (f) promoting relevant civil liberties and human rights considerations; (g) protecting vulnerable persons online; (h) educating the individual Internet user.
- **Strengthening capacity building activities.** Awareness-raising events could be followed-up with capacity-building activities, as appropriate. Potential activities could include: (a) assisting participating States in setting up Computer Emergency Response Teams and promoting the co-operation of these bodies; (b) organizing roundtables for cyber-security practitioners and decision makers; (c) issuing an annual publication providing answers to the year’s most pressing cyber security questions; (d) publishing a “Handbook” and/or Journal on Cyber Security; (e) facilitating law enforcement, judiciary and national security services exchanges of experience combined with technical training on investigation and electronic evidence; (f) exploring ways to expand criminal liability, and territorial jurisdiction to prosecute online exploitation and all forms of trafficking in human beings through the Internet
- **Supporting** international efforts, especially in the UN context, aimed at putting in place a global framework for dealing with cyber threats.

I. Background

Security in Afghanistan is inextricably linked with security in Central Asia and in the OSCE region as a whole. A number of threats stemming from Afghanistan are a source of serious concern for participating States. These include: the potential spill-over of continued insurgency, including possible infiltrations of combatants into Central Asia; the spread of violent extremism, fundamentalism and religious radicalism; terrorism; organized crime; trafficking (to and from Afghanistan) of arms, drugs/precursors and human beings. These threats are closely interrelated, and are inherently cross-dimensional.

Since 2003, when Afghanistan became an OSCE Partner for Co-operation, the Organization has been involved in a number of activities aimed at sharing with this Partner State OSCE core values and experience across all dimensions (mainly through inviting Afghans to various OSCE events). The profile of the OSCE's engagement with Afghanistan was enhanced in 2004-2005 when the Permanent Council responded positively to the Afghan Government's requests to send OSCE/ODIHR Election Support Teams to Afghanistan to assist in Presidential and Parliament elections accordingly.

The evolution of the situation in Afghanistan in recent years and an increased need for international assistance has prompted the OSCE to review its strategy toward this Partner State. Responding to the request of the Afghan Government, OSCE Foreign Ministers at the Madrid Ministerial Council adopted MC.DEC/4/07 on OSCE Engagement with Afghanistan, with a focus on assistance in the areas of border security, police and customs training, and combating drug trafficking. To date, this decision remains the main political framework for OSCE involvement in Afghanistan.

In consultation with the participating States, the Afghan Government and relevant international/regional organizations, in 2008 the Secretariat developed a Programme of Activities (16 extra-budgetary project proposals) on the implementation of MC.DEC/4/07. The emphasis was placed on key areas where the OSCE was able to provide an added-value contribution to relevant international efforts and Afghan Government strategies: border security and management, training of police and customs officers, and facilitation of cross-border co-operation and networking.

II. Current activities

The practical implementation of the Programme started in 2009 and is ongoing. Given the diverse and cross-cutting nature of the challenges faced by the Afghan authorities, the OSCE's response has involved a closely co-ordinated "teamwork" by different Secretariat units (OSG, Borders Team, SPMU, ATU, OCEEA, External Co-operation) and field operations, mainly in Central Asia.

A tangible contribution to the OSCE's work on Afghanistan was made by **ODIHR**, which deployed an Election Support Team to the 20 August 2009 presidential and provincial

council elections. The team deployed to Afghanistan from July to November, and produced a report containing recommendations for the improvement of future electoral processes. Prior to this deployment, ODIHR co-ordinated a series of activities to engage Afghan authorities and civil society groups with OSCE election-related commitments, to inform them of OSCE/ODIHR election observation methodology, and to discuss previous OSCE Election Support Team recommendations.

A number of other activities involving Afghan nationals were carried out under the OSCE Partnership Fund.

III. Co-operation with International Organizations

So far, the OSCE's co-ordination with international organizations has been carried out on an ad-hoc, case-by-case basis, mainly through information sharing and cross invitation to each other's events/meetings. It is an area where the OSCE could enhance its performance by improving co-operation with other international/regional actors, including on the basis of 1999 Platform for Cooperative Security.

One example of positive inter-institutional co-ordination was the preparation of the 2008 OSCE Programme of Actions: the Secretariat held consultations with key international organizations involved in Afghanistan (UNAMA, World Bank, WCO, UNODC, NATO/ISAF, EU, EUPOL, CSTO) and the Afghan Government to ensure that OSCE activities were consistent with international and national strategies. The Secretary General and other OSCE officials participated regularly in International Conferences and other international/regional events on Afghanistan (2008 Paris, 2008 SCO, 2008 The Hague and 2009 London Conferences).

Another example of positive co-ordination relates to ODIHR's interaction with partners in the field of election support. Before deploying the 2009 Election Support Team, ODIHR co-ordinated with all relevant stakeholders, including the UN Electoral Assistance Division (UN/EAD), UNAMA, UNDP, the European Commission, the European Delegation in Kabul, civil society groups, diplomatic representations in Kabul and international election support bodies operating in Afghanistan (NDI, IRI, IFES, USAID). Co-ordination included joining pre-deployment visits by the EU Election Observation Mission, holding lessons learned discussions from the 2004/2005 deployments with UN/EAD and UNDP/ELECT, and the exchange of letters between the OSCE Secretary General and NATO/ISAF, UNAMA and the Afghan authorities. This positive co-ordination continues with regular discussions between the OSCE/ODIHR and international as well as national election stakeholders.

IV. Gaps and Ways to Address Them

- **Political constraints**, stemming from different perceptions of the threats emanating from Afghanistan and ways to address them – and in particular whether border management, law enforcement training and counter narcotics efforts might involve limited project activity inside Afghanistan. A more robust OSCE engagement with Afghanistan would require increased political will to commit political support and resources. A possible OSCE summit with a focus, *inter alia*, on Afghanistan, could generate such momentum and support.

- **Internal co-ordination** among the Secretariat's thematic Units and between the Secretariat, Institutions and field operations must be further enhanced to streamline the planning and implementation process. The establishment of a Secretariat Afghan Task Force led by the Secretary General has been a step in ensuring internal co-ordination within the Secretariat. The CPC provides a co-ordination mechanism between Secretariat and relevant field operations. Other measures could be considered.
- **To consider the appointment of the CiO Special Representative on Afghanistan**, subject to consultations with the participating States and the Afghan Government on the specific mandate of the SR.
- **Improved co-ordination:**
 - **with all participating States**, through periodic inclusion of relevant aspects of Afghan-related issues onto the agendas of decision-making and consultative bodies (PrepCom, PC Committees) or ad-hoc meetings, including with the participation of donors. Afghan-related topics could also be more frequently added to the agendas of various OSCE meetings (seminars, workshops, training courses)
 - **with Central Asian States**, which border Afghanistan and host OSCE Field Operations involved in Afghan-related activities. An improved co-ordination mechanism – through relevant field operations and Secretariat - with the government agencies (borders, police, customs, counter-narcotics) dealing with Afghanistan, and also with a view to promote a coherent regional approach towards Afghanistan would be a valuable contribution.
 - **with Afghan authorities**, through identifying Afghan national liaison contacts in the Afghan government agencies. The recent appointment of a dedicated liaison officer in the Kazakh Embassy in Kabul has proved an effective measure, and it is important to sustain such practice in the long run.
 - **with international/regional organizations**. As mentioned above, to date the co-operation with other partner organizations on Afghanistan has taken place in the form of periodic meetings, including in the margins of different international conferences or events. A more structured and systematic approach would contribute to better co-ordination and greater synergy of efforts of various actors, including UN and the Afghan authorities, and would also assist in forging a more comprehensive regional framework to address Afghanistan-related issues.
 - Such an approach could be pursued, for example, through the establishment, in consultation with interested international organizations, of a **more regular framework (bilateral or multilateral) for information sharing and co-ordination of strategies** and resources on different aspects of TNT as they relate to Afghanistan.

A regular exchange of information between relevant Afghan Task Forces (analogue to OSCE) at the working/Secretariat level could be considered. To facilitate such exchanges, focal points could be identified in relevant partner organizations.

A more clear division of labour among different international organization might be especially relevant on such issues as the reform of law-enforcement agencies and training of Afghan law-enforcement personnel

V. Future activities

So far, the OSCE's engagement with Afghanistan has been confined mainly to the politico-military dimension (police, anti-narcotics, borders, customs) and electoral support, and delivered mainly on the territory of participating States (with the exception of the ODIHR ESTs) through the use of extra-budgetary resources. These activities have proved their relevance, and gained the support of the Afghan Government, which has expressed interest in their continuation. Athens MC.DEC/02/09 has, *inter alia*, called for an intensified implementation of the Madrid MC.DEC/04/07 on OSCE engagement with Afghanistan.

The following three key areas are suggested for enhanced OSCE engagement with Afghanistan:

- 1) Building on/expanding existing activities aimed at strengthening the borders between Central Asian participating States and Afghanistan through the training of police, border guards, and customs as well as promoting cross-border co-operation.**

In accordance with MC 04/07, the OSCE plans to continue providing assistance on strengthening borders between CA and Afghanistan through ExB projects, including with stronger Afghan participation. Subject to consensus by participating States, some of these projects could eventually be implemented in border areas in Afghanistan.

- The SPMU will continue to be engaged in training Afghan Police on counter-narcotics in Kazakhstan (Almaty), Russia (Domodedovo), Turkey (TADOC, Ankara) and Tajikistan (Dushanbe). These training courses provide an effective training platform and contribute to enhancing cross-border co-operation with Afghanistan and its neighbours. The OSCE stands ready to consider additional ideas and proposals on increasing police training for Afghan law-enforcement agencies, provided a relevant request and available resources are in place.
- The CPC Borders Team plans to use the ongoing ExB project "Patrol Programming and Leadership" (PPL), which has been ongoing since 2008 and is scheduled to conclude in 2011, as a vehicle to further engagement with Afghanistan. This project provides skills and knowledge necessary to build the capacity of the Tajik Department of Border Troops to detect and interdict illegal cross border movement across the Tajik/Afghan border, through the use of improved human surveillance and mobile groups.
- Subject to the agreement of the Tajik authorities and the availability of funds, an extension of the above is planned as ExB project "Tactical Patrolling and Surveillance for Afghan border police" (No.3 of the 2008 "Afghan Package"). This project aims at providing support for Afghan participation in tactical patrolling and analysis exercises, while strengthening cross border co-operation between Tajikistan and Afghanistan. The project would run for four months starting in autumn 2010 with a

budget of approximately euro 250,000, and would involve up to 16 Afghan border police officers.

- Upon completion of the two projects described above (No. 3 and the 2008-2011 PPL) in summer 2011, another joint follow-up project on tactical patrolling training and the renovation of training facilities near the border with Afghanistan could be carried out, with the participation of both Tajik border guards and Afghan border police. The purpose of this project would be to train up to 300 Afghan border police officers jointly with Tajik border guards on the Tajik side of the border for three years (from summer 2011). The estimated budget is approximately euro 2.5 million.
- In addition, conditional to the security situation and a consensus reached by the participating States, part of the field exercises and training foreseen under this project could take place concurrently on both sides of the border, with the participation of border officers from both countries to be mentored by OSCE experts. Such a “parallel” training would contribute to fostering operational co-operation between the two countries in the border area.
- The OSCE also plans to increase co-operation with the Afghan Customs Service. The Customs Training Facility in Bishkek (ongoing project No 6 from the “Afghan Package”) has recently agreed to co-operate closely with the Customs Academy in Kabul. Both trainees and trainers from the latter institution are going to take part in training exercises planned in Bishkek for summer 2010.
- Building on the successful implementation of the ongoing project “Customs Assistance in the Gorno-Badakshan region, Tajikistan” (No 5 of the “Afghan Package”), the co-operation between Tajik and Afghan Customs could be further strengthened in GBAO through additional joint training exercises for customs officers of both countries. Such joint training would focus on non-intrusive inspection and detection capacities for up to 60 Tajik and Afghan customs officers. Such a project expansion would last for about 17 months at a cost of approximately euro 1 million.
- Following the successful completion in 2009 of two OSCE pilot projects on Border and Customs Assistance in Turkmenistan (Projects No 1 and 2 of the “Afghan Package”), the OSCE plans to implement a follow-up phase to enhance the capacity of the State Border Service of Turkmenistan to detect and interdict illegal cross border movement through the use of improved human surveillance. The project could operate on a rotational basis and deliver various training activities in Ashgabat and at various border locations along Turkmenistan’s border with Afghanistan. In case of agreement of the Turkmen authorities and the availability of funds, this 15-month project could start in autumn 2010 with a budget of approximately euro 950,000.

2) **Continued election support by OSCE/ODIHR and technical expert assistance in long-term electoral reform.**

Should there be an explicit request from the Afghan authorities and agreement of participating States on the appropriate mandate, ODIHR could deliver a **more robust electoral support to Afghanistan**, including through supporting a strategy group, consisting primarily of Afghan election stakeholders, but also international actors and experts in developing a strategic long-term plan for electoral reform. The strategic plan for long-term

electoral reform could include issues such as the election calendar, voter registration, legislative reform, capacity building and sustainability. ODIHR could also play a supporting role by supplying technical experts to such a strategy group.

Another idea could be the organization of a conference by the OSCE, for example, in Central Asia, in order to discuss various aspects of the electoral reports on Afghan elections, including a review of the recommendations of all of the ODIHR Election Support Team reports and the reports of other organizations.

A possibility of **providing OSCE/ODIHR election support to the September Parliamentary elections** in Afghanistan could be considered in due time.

3) Developing new activities in the Economic and Environmental and Human Dimensions.

The International London Conference on Afghanistan on 28 January 2010 brought new opportunities for the OSCE's "Afghanistan agenda", going beyond the politico-military dimension. The Conference's main recommendation was to re-focus international efforts on the gradual transfer of responsibility to the Afghan Government ("Afghan Leadership") through increased assistance in national capacity building in different dimensions. Such a broad approach could also include enhanced regional co-operation, combating terrorism and drug trafficking, addressing violent extremism and corruption, promoting economic development and reconciliation, and promoting the rule of law and respect for human rights, including the rights of women.

These are all areas where the OSCE has unique expertise and could add value to international efforts. Therefore, it might be necessary to update the ongoing OSCE Afghan-related activities in line with the London recommendations.

All of these activities would follow the same principles as the original Afghan Package: close co-ordination with key stakeholders (Afghan, regional and international), added-valued, time-limited, funded mainly from ExBs.

Such new areas might include: sharing OSCE experience in reconciliation, combating trafficking in human beings, civilian capacity-building, gender equality, economic/environmental rehabilitation, cross-border trade facilitation, election support, including on electoral reform, promoting the rule of law, human rights, gender equality, and training for legislators. Broader involvement of OSCE institutions in implementation of these activities is essential.

Should such activities require additional resources or go out of the OSCE area, additional mandates and resources might be sought from participating States. An increased workload of OSCE activities on Afghanistan, involving enhanced co-ordination at all levels (intra- and inter-Organizational) and/or regional co-operation, might merit the consideration of the establishment of additional mechanism in Secretariat ("Task Force on Afghanistan" composed of representatives of different units, institutions and field operations, under the Secretary General's authority, along the lines of the 2006 Task Force on Organized Crime), in order to ensure more focused co-ordination with other executive structures and partner organizations and donors.

I. Background

Proliferation of weapons of mass destruction and their means of delivery constitutes a serious threat to international peace, security and stability, and there is increasing concern that WMD might be used by non-state actors. Combating nuclear terrorism is a vital issue also for the OSCE's participating States, and many have recently emphasized the need to step up OSCE activities to address this threat.

International non-proliferation efforts are based on the United Nations Security Council Resolution 1540 on Non-proliferation of Weapons of Mass Destruction (2004)¹¹, which imposes binding obligations on all states to establish domestic controls to prevent the proliferation of nuclear, chemical and biological weapons and their means of delivery, including by establishing appropriate controls over related materials. It also encourages enhanced international co-operation on such efforts, in accordance with and promoting universal adherence to existing international non-proliferation treaties. In addition, the Resolution established a special 1540 Committee that reports to the Security Council on 1540 implementation. In 2008, the Security Council adopted Resolution 1810, which underscores the potential of regional organizations in promoting the implementation of UNSCR 1540.

At the OSCE level, the participating States' commitment to combating the proliferation of weapons of mass destruction was first outlined in the 1994 OSCE Principles Governing Non-Proliferation (DOC.FSC/6/96). In 2006, with the adoption of FSC Decision 10/06 on Supporting National Implementation of UN Security Council Resolution 1540, the participating States agreed to "*hold further exchanges of views [...] with the goal, inter alia, of furthering UN efforts by promoting lessons learned, sharing experiences and facilitating the identification of assistance needs for national implementation.*" This was endorsed by MC Decision 10/06.

More recently, Athens MC DEC.16/09 on Issues Relevant to the FSC called on the FSC, in 2010, to "*facilitate, where appropriate, the fulfilment by the OSCE participating States of the provisions of UNSCR 1540 (2004), UNSCR 1673(2006) and UNSCR 1810 (2008)*". Furthermore, the Athens Ministerial Declaration on Non-proliferation (MC.DOC/5/09) pledged "*continued support to the ongoing UNSCR 1540 (2004) comprehensive review process, Committee's and regional efforts to facilitate its implementation, including through providing effective assistance to those States that require it*".

As the world's largest regional security organization, the OSCE could make a significant contribution to furthering 1540 implementation. Throughout the UNSCR 1540 Review process, the OSCE's development of Best Practice Guides was praised by a significant number of UN member states and international organizations as a useful input from the OSCE to the global process. It also became clear that in its own area of application awareness

¹¹ UNSCR 1540 was followed-up by UNSCR 1673 (2006), which reiterated the previous resolution and expressed the interest of the Security Council in intensifying its efforts to promote its full implementation

raising among high level policy-makers and practitioners about 1540 commitments¹² is needed. Awareness raising might be followed up by capacity building through providing practical assistance to pS to improve or develop necessary legislation. Such activities could help raise the international bar for counter-proliferation through (*inter alia*) improved national legislation, effective enforcement of that legislation, improved export control provisions and a more level playing field internationally, so that proliferators find it more difficult to use certain states with lax legislation and implementation as ‘proliferation havens’.

The Athens Ministerial Council documents provided for the necessary political mandate to develop OSCE action on non-proliferation. If the OSCE is to make the most of its potential to contribute effectively to UN efforts in this area, there is an urgent need to enhance the Secretariat’s expertise in 1540. To this end, a special post of a 1540 Adviser, to be funded by extra-budgetary contributions, has been established in the CPC. The Organization already has a number of thematic units (ATU, SPMU, Border Unit) than can provide related expertise. In addition, the field operations can serve as a tool for awareness-raising and practical assistance. Together, this network can form a significant asset to the participating States in their efforts to enhance 1540 implementation.

II. Current Activities

Based on experiences gained in the OSCE region in the national implementation of Resolution 1540, a number of participating States have launched the development of an OSCE Handbook of Best Practice Guides for Implementation of UNSCR 1540. When complete, the Handbook will consist of five best practice guides, intended to assist in the development of national action plans by OSCE participating States and Partners for Co-operation. These best practices could be useful also for other UN member states seeking further information on “appropriate controls” in the area of border security, export control and physical protection of biological, chemical, nuclear and related technologies. The first Best Practice Guide, addressing “Export Controls and Transshipment,” was endorsed by FSC Decision 07/09. Future Guides will focus on:

- “Practices prohibiting non-state actors from acquisition and use of WMD”;
- “Effective accounting and security of WMD materials”;
- “Developing physical protection of WMD materials”;
- “Establishing border controls in relation to WMD materials”.

III. Co-operation with International Organizations

The United Nations and its 1540 Committee have a leading role in promoting UNSCR 1540 implementation. The OSCE closely follows the work of the 1540 Committee and regularly reports therein on its own activities at the regional level.

Enhanced OSCE action in this area will require pro-active co-ordination and consultations also with other relevant actors, including the IAEA, the OPCW and specialized NGOs, in

¹² This could be done at two levels: high level CiO contacts in participating States to increase their knowledge about 1540 commitments and practical workshops for implementers.

order to build partnerships and identify issue areas where the OSCE could best contribute to 1540 implementation.

IV. Gaps and Ways to Address them

According to 1540 Committee experts, the main challenge that a number of participating States are facing is the application of the obligations outlined in the Resolution and lack of national legislation. These gaps are known through the implementation matrices produced by the 1540 Committee experts. In particular, enactment of legislation on biological and chemical components accounting, security and physical protection is least well implemented. In this context, a number of the OSCE participating States would benefit from capacity building and assistance with updating their national legislation.

At the organizational level, the OSCE does not yet possess extensive expertise or institutional memory on 1540 implementation, meaning that the Organization must rely on partnership with other actors to ensure the effectiveness of its own activities. Also internal co-operation and co-ordination among active participating States and within the Secretariat should be established to involve all thematic units dealing with trans-border crime, border management, terrorism, trafficking, etc., which, if tied together in the right way, could form a significant asset to participating States in their efforts to enhance 1540 implementation.

The OSCE field operations could be used to support raising awareness on non-proliferation issues in their host countries and implementing concrete projects to address proliferation-related issues. Specialized training for politico-military focal points in the field operations could be organized in order to gain maximum effect through these channels.

V. Future Activities

UNSCR 1810 put a significant emphasis on the role that could be played by regional organizations in the implementation of UNSCR 1540. Given the constantly increasing attention to this issue, including at the highest political level, it is likely to remain high on the OSCE's list of priorities. An event by the FSC, which is planned for October 2010, is called to provide political guidance from participating States, including clearer priorities for relevant activities by the OSCE.

Such activities might include:

- Updating the 1994 Principles Governing Non-proliferation. Some participating States have expressed an interest in updating the 1994 Principles Governing Non-proliferation in order to reflect developments since their adoption.
- Assisting participating States in developing national action plans and national legislation. A four-year extra-budgetary project to Support Regional Implementation of UNSCR 1540 has been created by the CPC with the aim of strengthening OSCE expertise and capacities to transform existing political taskings into concrete assistance activities and support for global processes. The project would assist participating States in producing national action plans and establishing new legislation required for 1540 implementation. The project will be implemented by a 1540 Adviser in the Secretariat (CPC). In order for this activity to be successful, there is a need to generate political will to improve

participating States' compliance with UNSCR 1540 and to encourage the participating States to seek assistance from the OSCE executive structures.

- Awareness-raising. The UN Office for Disarmament and the Chair of the 1540 Committee have suggested that a series of practical workshops in Central Asia and Eastern Europe could be organized together with the OSCE to discuss specific implementation gaps and challenges to set the basis for the targeted work with individual countries on their specific challenges.

Depending on the outcome of the aforementioned activities, the interest of participating States and the availability of funds and resources, possible additional programmatic measures could also include:

- Providing practical assistance to participating States upon their request. An assistance mechanism similar to those developed to address SALW and SCA could be created. The OSCE could, upon request from participating States, provide practical assistance in promoting non-proliferation. Projects could be carried out in co-operation with other international organizations and, depending on their mandates, the OSCE Field Operations could also contribute to their planning and implementation. Assistance could be provided in a few niche areas where the OSCE could bring value-added, such as border controls, with courses to be provided by the OSCE Border Management Staff College.
- The OSCE could also deliver training to foster co-operation among police, prosecutors, customs, border control, intelligence agencies and military authorities to improve the legal, technical and administrative basis for sound and effective national implementation of non-proliferation legislation and its increased harmonization. In addition, the OSCE could facilitate the broad engagement of technical expertise resident in civil society. Assistance could be provided to pertinent civil society organizations as these can play an important role by functioning as clearing houses for information for states and international organizations and a pool of expertise for states to draw from. As with existing assistance mechanisms, such projects would be financed by extra-budgetary funds.

From the managerial perspective, in case the OSCE engagement with UNSCR 1540 issues proves to be a useful tool at the national, regional and global levels, the respective workload is likely to increase significantly, requiring allocation of additional human resources to the Secretariat. In this situation an option of establishing a contracted “non-proliferation position” within the Secretariat, rather than on an ExB or secondment basis, should not be ruled out.

PART 2: CONCLUSIONS AND RECOMMENDATIONS

Transnational threats by nature are dynamic and constantly evolving. To be effective, responses to such threats must be equally dynamic, flexible and coherent. While the decentralized nature of the OSCE offers the participating States a high degree of flexibility in adapting to evolving needs and tasks, it also complicates efforts to promote co-ordination and coherence.

Field operations often launch activities and projects without taking due account of similar work conducted by the Secretariat's thematic units or the Institutions. Similarly, the Secretariat's Units and the Institutions do not always take maximum advantage of each other's experience when planning their own activities.

Brussels Ministerial Decision 18/06 provided the Secretary General with the responsibility to "*ensure programmatic co-ordination between the Secretariat, institutions and field operations, as well as between the field operations, while respecting their mandates and mandates assigned to the fund managers by the participating States*". This role was further endorsed by the Athens Ministerial Decision 02/09 which, inter alia, "*requests the Secretary General to explore ways to further strengthen programmatic co-ordination between the OSCE executive structures, as set in MC.DEC.18/06, with particular focus on the OSCE's multidimensional activities to address transnational threats to security*". Yet these mandates have not been accompanied by the practical tools necessary to ensure such co-ordination.

Participating States may wish to consider ways to reinforce the co-ordination role of the Secretary General, inter alia, through the establishment of mechanisms for joint planning and implementation of activities that fall under the mandates of different structures, while preserving the overall autonomy and mandates of the Institutions and the Field Operations.

The Brussels MC.DEC/18/06 also tasked the Secretary General with "*bringing to the attention of the Permanent Council or the Forum for Security Co-operation (FSC), in consultation with the respective Chairmanship, any matter he/she deems relevant to his/her mandate.*" It also tasked him "*to contribute to, and participating in, the debates on any of the agenda items, including the review of current issues, inter alia, by providing background information, analysis and advice*". In order to fulfil this mandate with respect to the Organization's efforts to address transnational threats, the Secretary General must be able to identify emerging threats, understand the evolving inter-linkages between various strands of transnational threats, and recommend necessary adjustments in the Organization's approach. This, in turn, would need to be underpinned by an analytical capacity that currently does not exist. Similarly, to remain effective over time, OSCE thematic experts need the ability to adapt their responses to the evolving tools and methods employed by the perpetrators of transnational threats (including in cyberspace). They need to be able to develop effective forms of interaction with other international actors, and to cope with the reality that transnational threats do not recognize the borders of the OSCE area.

To achieve these goals, the following steps might be considered. While some can be undertaken within the existing authority of the Secretary General, others would require additional political decisions and/or resources to be provided by the participating States:

Within the existing mandate of the Secretary General:

- Include TNT-related issues as a permanent agenda item on **the agenda of regular meetings of Heads of Institutions and Heads of Missions**, or arrange special TNT-focused meetings, for example, in the margins of the ASRC.
- Building on the positive experience of the 2006 Task Force on Organized Crime, **establish a Task Force on Transnational Threats** under the authority of the Secretary General, which would include representatives of the Secretariat's Thematic Units, CPC, Field Operations and Institutions (TNT focal points). The Group, **supported by the TNT Analytical Unit and a TNT Director/Coordinator** (if established), would regularly conduct its meetings (monthly or when necessary) at the Secretariat to review the OSCE's work on transnational threats, discuss and adopt common approaches and operational strategies/plans, plan a joint calendar of events. The Group would closely co-ordinate its activity with the Security Committee, including through regular reports to participating States.

At the level of participating States:

- **Consider reviewing the 2003 OSCE Maastricht Strategy to Address Threats to Security and Stability in the 21st Century** with a view to adapting it in line with the evolution of the nature of threats, and augmenting, if necessary, the list of threats the OSCE is tasked to address
- **Organize a series of Conferences/Seminars/Workshops on each TNT thematic area** in order to clarify the political priorities of the OSCE participating States and ways to address them by the OSCE. Some conferences are already planned for this year (Anti-Terrorism, Illegal Drugs and Precursors etc.), while others might be considered at a later stage. The possible follow-up with recommendations or even decisions on each of the topic would be able to provide a coherent position of the OSCE community on these issues
- Consider establishment of the **Cyber Security Unit** in the Secretariat
- Consider enhancing **anti-drugs capacities** in the SPMU
- Consider the establishment of **an analytical/threat assessment capacity (Unit)** within the Secretariat, tasked with providing broader assessment, identifying emerging transnational threats, overall trends related to their evolution and the links between their various aspects. Such a unit would be directly subordinated to the TNT Director/Coordinator (see below). The establishment of such a Unit would contribute to enabling Secretary General to perform his mandate under the Brussels MC.DEC/18/06 to ensure programmatic co-ordination between different executive structures, particularly in the area of transnational threats, and to bring to the attention of the PC and/or FSC matters which he/she deems relevant to his/her mandate
- Consider the establishment of a **TNT Directorate** within the Secretariat, which would consolidate the work of the existing thematic units and also possible new structures (Analytical/Threat Assessment Unit, Cyber Security Unit and enhanced anti-drugs capacities in the SPMU), with a mandate to co-ordinate the Organization's TNT focal point network and support programmatic activities aimed at addressing TNT carried out

by all OSCE executive structures. The Secretariat would be ready to present its concrete ideas on the organizational chart of such a Directorate

- **Alternatively**, if the participating States wish to stop short of formal vertical integration of thematic units, **this role could be played by a TNT Coordinator** (P5 or senior secondee) as a head of an Analytical/Threat Assessment Unit. The TNT Director/Coordinator would also serve as a primary focal point for liaising on TNT issues with other international organizations, NGOs and academic institutions
- Re-examine the existing mandates/decisions pertaining to the OSCE's activities in different thematic areas related to TNT. As most mandates of the existing thematic activities are based on ad-hoc decisions dispersed in various OSCE documents, **it might be necessary to consider reviewing and adopting (or updating, as appropriate) the mandates of the Thematic Units** of the Secretariat through a special PC or/and FSC decision/s. The Thematic Units should become **the central co-ordination mechanism** for the thematic work on transnational threats conducted by all executive structures, including Field Operations and Institutions. The Thematic Units would provide expert support to the thematic activities of all executive structures
- In order to facilitate this work, **to establish a network of TNT focal points in the Institutions** to be supervised by the Secretariat's TNT Coordinator
- Consider the further enhancement of the support provided by the OSCE field operations to the host states through the establishment of seconded **"TNT Adviser/Officer"** positions in some or all of the OSCE field operations. These Advisers/Officers would be tasked to work closely and liaise with the local authorities and international and regional organizations as well as with bilateral donors in developing programmes to address the needs of the participating States and facilitate regional co-operation. These officers would also contribute to the work of the Secretariat's **TNT Task Force** in developing comprehensive trend analysis on transnational threats. An alternative could be the establishment of a single **TNT Adviser** position for each OSCE region.
- Consider the allocation of increased resources to certain areas of work to address TNT.

Improving Co-operation with International Organizations:

- Intensify practical Secretariat-level co-operation with partner international organizations (UN, EU, NATO, COE, CSTO, CIS, CARICC etc) on TNT-related issues, including those related to engagement with Afghanistan: convene expert meetings on different topics related to TNT; conduct joint research, analysis, information and best-practice sharing, co-ordination of programmes and plans of actions, draft common strategies, working plans, cross-participation in events etc. To facilitate such exchanges, focal points could be identified in relevant partner organizations with a view to forming an international network of TNT focal points.
- Consider the replication of the positive experience of *the Alliance against Trafficking in Persons* on other areas of work related to TNT. This approach could provide an organizational framework to gather leading international and regional organizations, private sector, think tank organizations, NGOs and civil society. Such a framework could provide an important tool for building strategic partnership between traditional actors (such as international organizations) and members of the private sector and civil society.

The structure could be initiated with a high-level conference inviting all the main stakeholders to launch a common informal platform for consolidating existing partnerships and providing an additional tool to assist participating States in meeting the challenges of evolving threats. Furthermore, this consultation mechanism could be complemented by a **network of international experts** from different international organizations and national experts from participating States. **Annual meetings of experts** on different types of threats could be organized to exchange knowledge and practices in addressing TNTs, to establish shared priorities and to undertake joint initiatives. It could also contribute to developing national and regional strategies and tailored assistance programmes for participating States. The cost of this initiative and of its regular operation should be part of the Unified budget of the Secretariat.

- To revisit the idea of **an Ad-Hoc Consultative Mechanism** with other International Organizations on TNT issues as envisioned by the 2003 Maastricht Strategy to Address Threats to Security and Stability in the 21st Century.

ANNEX 1 - A suggested list of possible decisions by participating States in thematic areas

Preventing and Combating Terrorism

- Adoption of a comprehensive mandate on OSCE overall anti-terrorist activities, including on new areas
- Consideration of allocation of additional resources (during Programme Outline discussion and UB budget process)

Fighting Organized Crime

- A review of an OSCE mandate on the issues related to organized crime, including on anti-corruption activities, money laundering and terrorist financing
- To consider the adoption of an OSCE strategic document/action plan on counter-narcotics efforts
- To consider enhancing anti-drugs capacities of the SPMU (renaming SPM/Anti-Drug Unit or Organized Crime Unit could be considered)

Promoting Cyber Security

- To consider elaboration of an OSCE strategic document on a comprehensive approach towards cyber security
- To consider establishment of a Cyber Security Unit within the Secretariat

Addressing Threats Stemming from Afghanistan

- To consider the adoption of a new decision on OSCE engagement with Afghanistan (“Madrid-2”) to reflect the evolution of the situation in and around Afghanistan and a possible OSCE contribution to the international efforts.
- Establishment of an Afghan Task Force under the Secretary General guidance, comprising of the relevant executive structures’ representatives
- To consider appointment of the CiO Special Representative on Afghanistan

Preventing the Proliferation of WMD in the context of UNSCR 1540

- Start-off of consultations on updating the 1994 Principles of Non-Proliferation