Public-Private Expert Workshop for South-Eastern Europe
on Suppressing Terrorist Financing and
Countering Violent Extremism and Radicalization
that Lead to Terrorism

*8-10 December 2010
Hosted in the Parliament of Bosnia and Herzegovina
Sarajevo, Bosnia and Herzegovina*

Organized thanks to an extra-budgetary contribution from the United States of America and with the support from the Charity Commission for England and Wales

osce
United States Mission to the OSCE

CHARITY COMMISSION

Findings and Suggestions
Advanced during the Workshop

On 8-10 December 2010 the OSCE Action against Terrorism Unit (ATU) organized a sub-regional workshop for South-Eastern Europe on public-private partnerships in countering terrorism, in line with OSCE Ministerial Council Decision No. 5/07 on *Public-Private Partnerships in Countering Terrorism*.

The workshop brought together over 110 experts from 15 OSCE participating States, six international structures and 32 private sector organizations, to discuss ways to improve public-private co-operation to block channels of terrorist financing and to counter violent extremism and radicalization that lead to terrorism, while upholding human rights and fundamental freedoms.

The event, hosted in the Parliament of Bosnia and Herzegovina in Sarajevo, in co-operation with the Ministry of Security of Bosnia and Herzegovina, was organized with the support of the OSCE Mission to Bosnia and Herzegovina, thanks to an extra budgetary contribution from the United States of America and in partnership with the Charity Commission for England and Wales.

The ATU has subsequently compiled the present summary of findings and suggestions advanced during the workshop. **These findings and suggestions should not be understood as an alternative to existing internationally agreed recommendations**, notably the 40+9 Recommendations against Money Laundering and Terrorism Financing (ML/TF) and the related guidance materials published by the Financial Action Task Force (FATF).

Neither should this summary be interpreted as official OSCE recommendations based on a consensus decision, or the official position of any particular OSCE participating State; it reflects opinions expressed individually by workshop participants.

It is understood that state authorities competent over issues related to ML/FT and violent extremism and radicalization that lead to terrorism (VERLT) may vary from one country to the other. In this regard, it was underscored that governments should carefully consider and select which state authorities to involve and how to effectively achieve inter-agency co-ordination.

Session 1: Public Oversight of and Partnerships with Financial Institutions

1. Anti-money laundering and combating terrorist financing (AML/CFT) legislation should be drafted in consultation with all relevant stakeholders, including the industry.

2. State authorities should ensure adequate confidentiality and protection of obligated entities from liability *vis à vis* third parties in the context of reporting on suspicious transactions.

3. Financial institutions expect from state authorities more communication, reciprocity in information sharing, proportionality in the design and imposition of AML/CFT measures, transparency and commitment to co-operative relationships.

4. State authorities must do more to reach out to financial institutions, whether to provide guidance on vulnerabilities of financial products/services, typologies of abuses, risk indicators, or to give feedback on their reporting of suspicious transactions.

5. State authorities should consider a variety of outreach and capacity building activities directed towards financial institutions, e.g. written materials disseminated by different channels, special notifications/alerts, seminars and conferences, training workshops.

6. State authorities may consider options for enhanced reciprocal information exchange with industry stakeholders on confidential issues, e.g. through regular meetings with vetted industry representatives.

7. More efforts are required to mitigate ML/TF risks in informal money transfer systems, such as those used for remittances, including through public awareness raising and community outreach.

Session 2: Public Oversight of and Partnerships with Designated Non-Financial Businesses and Professions (DNFBPs)

8. Supervision of DNFBPs should be risk-based as per FATF's risk based approach guidance. The identification of DNFBPs and the adoption of a risk-based approach to their supervision should be defined by law.

9. State authorities and private sector stakeholders should join forces to achieve, maintain and disseminate a clear understanding of the ML/TF risks facing each designated non-financial business or profession in each country. This is a pre-requisite for effective risk-based supervision.

10. ALM/CFT measures for DNFBPs should be tailored and proportionate, taking into account different criteria (e.g. specificities, size and vulnerabilities of each business or profession). In particular, regulators must be sensitive to legal privileges and address specific concerns of some DNFBPs, e.g. attorney-client relationship.

11. DNFBPs should be consulted in the process of defining and if necessary re-adjusting their respective AML/CFT regime, in order to increase buy-in and enhance compliance.

12. To be effective, relationships between supervisors and DNFBPs should be clearly defined, based on written agreements, regular interaction and a constructive spirit of co-operation between equal partners.

13. Self-regulation of DNFBPs can be empowered through national and international sector associations. Affiliation with these associations should be strongly encouraged where not made compulsory by law.

Session 3: Government Oversight of the Non-Profit Sector and Enforcement Actions

14. The degree of exposure and vulnerability of non-profit organizations (NPOs) to abuse for terrorist financing must be factually established through typology work, risk assessment and

mapping of the non-profit sector in each country. This should not be a one-off but rather a dynamic exercise, best conducted in co-operation with the sector itself.

15. All countries must ultimately have an effective system in place to prevent, detect and take firm action against ML/FT abuse of NPOs, without unduly disrupting or discouraging not-for-profit activities.

16. State authorities should adopt a proportionate and non-discriminatory approach in regulating and overseeing NPOs, which balances legally defined concerns, such as security, against the necessary facilitation and promotion of the fundamental freedom of association.

17. The ultimate objective of NPO regulation and oversight should be to protect the non-profit sector, not to police or curb it. Curtailing the non-profit sector would actually be counter productive from a broader counter-terrorism perspective since NPOs, in particular humanitarian organizations, can play an essential role in addressing the factors conducive to terrorism.

18. Effective regulation, oversight of and engagement with the non-profit sector is best achieved through a comprehensive policy aiming to develop and strengthen the non-profit sector and which covers a wide range of risks, rather than terrorism financing only.

19. State authorities should seek and welcome the input from NPOs in the process of public policy formulation, legislative drafting and production of guidance materials, to ensure that compulsory or recommended AML/CFT measures are adapted to the reality of their non-profit sector (e.g. size of the sector, variety of the sector in terms of purpose and size of the NPOs, concerns, constraints, existing procedures that can be built on).

20. Obliging NPOs to process their financial transactions through banking institutions should not be an excuse for state authorities to simply discharge their supervisory duties *vis à vis* NPOs on banking institutions. The banking and non-profit sectors should be jointly engaged by state authorities in a multi-stakeholder discussion on the terrorism financing risk faced by NPOs.

21. The objective of enforcement should be to restore the integrity of the NPO involved in a ML/TF case and allow legitimate non-profit activities to carry on. When and where an enforcement action is required, state authorities should aim for a "surgical" intervention, targeting precisely and remedying the cause(s) of abuse, rather than closing down the whole NPO, unless it was a sham organization established for criminal purposes.

Session 4: Self-Regulation and Good Governance Capacity Building of the Non-Profit Sector

22. It is in the NPOs' own interest to protect themselves and the reputation of their sector from harm. State authorities should make them aware of terrorist financing and other criminal risks, and encourage them to take preventive action at individual level or in group.

23. State authorities should do more to engage in regular and inclusive dialogue and build trust with NPOs, recognizing them as equal and important for the establishing of sustainable democracies. NPOs should be open to constructive engagement and overcome initial distrust. Building trust and understanding through dialogue will ultimately provide a basis for concrete partnerships.

24. State authorities should actively encourage and invest in supporting NPO self-regulation to increase transparency and accountability. Regulation and self-regulation are complementary, not mutually exclusive; adequate regulation in scope, depth and clarity is actually an enabling force for self-regulation.

25. NPOs' willingness to register with state authorities (if not made compulsory by law) and voluntary compliance with higher standard of transparency/accountability should be rewarded through incentives, for instance tax relief and public benefit status.

26. The intended beneficiaries of charitable organizations should be brought into accountability models used by the non-profit sector.

27. NPOs, with support from state authorities, should facilitate the establishment of, and engage with umbrella NPOs representing all or part of the non-profit sector, at the national, regional or international levels. This would facilitate two-way interaction between the sector and state authorities, including collection of feedback, dissemination of guidance, and facilitation of training.

28. NPOs, with support from state authorities, should facilitate the establishment of, and engage with independent watchdogs (non governmental and non-profit organizations themselves) working as auditors/certifiers and whistle blowers within the non-profit sector at the national, regional or international levels.

29. State authorities and NPOs should join forces to educate donors and the broader public in terms of quality/accountability standards and the need to "know your charity". Pooling resources and making the most of traditional and new media will increase the impact of awareness raising campaigns.

30. NPOs should do more than pay lip service to transparency and actually value accountability as a mean to increase their quality and effectiveness. They should seek and utilize proactively good governance best practices for the non profit sector.

Session 5: Understanding the Challenge of Countering Violent Extremism and Radicalization that Lead to Terrorism

31. VERLT result from a complex interplay of various factors and therefore counteracting these phenomena requires a comprehensive and inclusive approach involving various stakeholders in different fields (e.g. politics, media, and youth) from both the public and private sectors.

32. It is imperative that policies and measures to counter VERLT be devised and implemented in conformity with international human rights law and the rule of law. There should be no unnecessary and disproportionate restrictions to, *inter alia*, the rights to equality and non-discrimination, privacy, freedom of thought, conscience and religion, and freedoms of expression and association.

33. Importantly, state authorities should carefully distinguish extremism and radicalism from *violent* extremism and radicalization that *lead to terrorism*. This boundary should be defined by Law and ascertained through due process by the judiciary, in accordance with international human rights law.

34. To be effective and sustainable, national approaches to countering VERLT should combine policies and measures both at the macro and micro levels – at the nation-wide and local levels.

35. At the macro level, countering VERLT is inextricable from the need to promote non-violent, democratic and inclusive societies. State authorities should consider efforts to combat discrimination as an integral part of efforts to prevent VERLT.

36. At the micro level, it is particularly important to invest in concrete and sustainable grassroots projects by municipalities, police and NGOs, and to ensure long-term monitoring beyond project completion.

37. Donor countries should consider how to mainstream counter VERLT objectives in their bilateral or multilateral development assistance programmes.

38. Policies and measures to counter VERLT should be based on scientific research and specific intelligence so as to avoid reliance on stereotypical assumptions.

39. State authorities should avoid discriminatory practices such as profiling of certain racial, ethnic or religious groups, which result in stigmatization, alienation, and mistrust of the State, proving ultimately to be counter-productive.

40. Factors making individuals and groups vulnerable to radicalization should be identified and addressed. Grievances, whether perceived or factually established, should be taken seriously. Vulnerable groups should be engaged with in a tailored way. Special attention should be paid to impressionable youth as well as to inmates during and after their incarceration.

41. It is incumbent on state authorities to reach out to non-governmental stakeholders and start a dialogue on VERLT in all its forms and manifestations, to exchange views and information, overcome bias and gradually build trust. Dialogue should however always be backed with concrete actions.

42. State authorities should be particularly cautious and sensitive when dealing with forms of violent extremism and radicalization that abuse religious dogmas to provide justification and legitimacy in their narratives. State authorities should be careful about the terminology they use and reject the use of inappropriate terminology by others, e.g. in the Media.

43. Training programmes should be established for security sector stakeholders, at both national and local levels, to improve their understanding of VERLT related challenges and their awareness of good practices and pitfalls to avoid.

44. Governments should make more and better use of their police in a wide range of preventive and outreach activities.

Session 6: International Experiences in Countering Violent Extremism and Radicalization that Lead to Terrorism

45. There is no one-size-fits-all solution: strategies, policies and measures to counter VERLT should be tailored to specific settings. Nevertheless, most if not all countries face some manifestations of violent extremism and should exchange experience and learn from each other.

46. There should be a clear policy and legal framework in place that provides state authorities with a wide range of options to choose from in order to take comprehensive and proportionate action against VERLT, from prevention to prosecution.

47. Violent extremist and terrorist propaganda can be highly versatile, subtle and sophisticated in the supports/media used (e.g. music) to target specific audiences (e.g. schoolchildren). State authorities, in particular law enforcement agencies, should keep pace with trends and commission/build on scientific research to inform their work.

48. Propaganda and recruitment operations are a double-edge sword for violent extremist and terrorist groups as it requires them to move into the open and get exposed to law enforcement and intelligence. State authorities should make the most of this opportunity, within the confines of the Law, to learn about and monitor suspected groups. This is particularly relevant for websites containing materials bordering on the illegal and where the outcome of a legal action might be uncertain, as well as websites which are hosted in another jurisdiction.

49. The overarching ideological objective in countering VERLT should be the rejection of violence by all groups and individuals in society. All forms of *violent* extremism should be tackled with equal firmness whether or not related to terrorism.

50. Stakeholders should focus on disaggregating grievances and demands from the advocacy and glorification of violence. The latter should be firmly condemned, while space is effectively provided for free expression and discussion of ideas/concerns within the boundaries set by Law, in accordance with international human rights law and media freedom standards.

51. Governments, through relevant state authorities and in partnership with private sector stakeholders (business community, civil society and the Media), should undertake preventive measures on the social, educational, communication, and cultural fronts.

52. Public-private partnerships are particularly instrumental to build up the "resistance" of vulnerable communities, empower counter voices, and promote self-regulation (e.g. of the Media).

53. Active solidarity with victims of terrorism to counter their dehumanization and highlight the harmful reality of terrorist violence is among the most powerful ways to counter violent extremist and terrorist propaganda and recruitment.

54. Governments should run assistance programmes to encourage individuals to drop out from violent extremist groups, de-radicalize and durably reintegrate society.

55. Democratic and community policing are key foundations for an effective role of the police in countering VERLT. Police should be transformed from a force into a service, not only respecting but also actively protecting human rights, with an emphasis on building understanding and trusted relationships with communities for crime prevention. To be effective, such reform requires strategic recognition, adoption of a Law on police and the development of specific tools, such as e.g. community policing officers and community advisory groups.

Session 7: Building Partnerships – Empowering Counter Voices

56. Civil society should be galvanized and empowered to challenge violent extremist and terrorist narratives and to engage with vulnerable groups/individuals.

57. In partnering with civil society, the media, religious institutions and other private sector stakeholders, state authorities should respect the independence and preserve the credibility of their partners. Likewise, international initiatives should focus on stimulating and supporting locally owned projects, in particular at grassroots level.

58. Religious institutions and leaders have the moral authority and duty to promote dialogue mutual respect and tolerance, and to publicly denounce terrorism and violent extremism.

59. Religious institutions/leaders and state authorities should engage constructively to denounce violence as well as to protect and promote freedom of thought, conscience and religion.

60. Acts of violent extremism and terrorism, especially against religious sites or figures, should be promptly, publicly and jointly denounced by religious leaders of all faiths, (local) authorities and other relevant institutions, to demonstrate cohesion and determination in the face of terrorism.

61. Wherever and whenever VERLT narratives build on perverse interpretations of religious tenets, these abuses should be highlighted and unequivocally challenged. Who is best placed to challenge these abuses must be carefully considered, to avoid giving inadvertently credibility to violent extremists and terrorists.

62. The "private face" of terrorists and violent extremists should be exposed to discredit and demystify them. Properly challenging them in public can expose their ignorance and ideological inconsistencies. Deradicalized individuals can be called upon to testify about the real agenda, rivalries among terrorists and violent extremists, as well as inconsistencies between their prescriptive rhetoric and their actual behaviour.

63. De-radicalization is ultimately a personal process but it can be catalyzed through constructive engagement and offering opportunities for reintegration in society. Vulnerable and radicalized individuals should be provided with the knowledge and skills to reach by themselves the realization that they are/were misled.

64. Women's engagement in countering VERLT should be actively encouraged and supported. Women are in a unique position to help combat VERLT through action at the community level, as they are situated at the critical nexus between family and society. Women can act as network for early warning and effective outreach towards vulnerable persons, in particular youth. Given their role in education, women are a critical vector to durably change attitudes, especially with regard to the use of violence.

65. Associations of victims of terrorism should be supported by state authorities and private sector stakeholders (civil society and business community) to give back a voice to victims and empower them as a counter VERLT force. Efforts should focus in particular on building their communication capacity, both in terms of skills and variety of outreach vectors (partnership with Media, Internet presence, TV campaign, commemorative events, visit to schools, etc).

66. Associations of victims of terrorism should network at the national, regional and international levels to share best practices on public outreach, pool resources, and raise their profile in society, with the media and state authorities.

Session 8: The Role of the Internet and Media in Countering Violent Extremism and Radicalization that Lead to Terrorism

67. Policies and measures to counter terrorist abuse of the Internet and the Media should balance the need to protect the free and global nature of the Internet and the independence of the Media, uphold freedom of expression, right to access information and the free flow of information, and take into account the interests of economic operators.

68. Close public-private co-operation is needed to both prevent (e.g. awareness raising, sharing of expertise, protecting critical information infrastructure, researching and monitoring) and react (e.g. reporting, freezing of evidence, restoring of infrastructure) to terrorist use of the Internet. Different mechanisms/initiatives should involve different stakeholders, whether Internet Service Providers (ISPs), hardware/software providers, NGOs, individual internet users, etc.

69. Countries should establish an effective interface between law enforcement agencies and ISPs with single points of contact and clear communication lines, in accordance with national legislation and international media standards.

70. Public-private dialogue and co-operation should address the issue of possible ISP liability towards their customers when ISPs are requested by state authorities to take down online materials or stop hosting websites. A possible solution could be an adequate provision in the contract between ISPs and their customers.

71. Hotlines should be established to allow every Internet user to report suspicious online content to ISPs and/or to relevant state authorities. Such hotlines can help foster a spirit of Internet citizenship among Internet users.

72. Public-private co-operation in preventing and countering the abuse of the Internet by terrorists should not result in an outsourcing and unregulated "privatization" of censorship. Individual Internet users should be empowered to the maximum extent to decide what content they want to access. There should be effective remedies available and due process to guarantee that the lawfulness of online content is ultimately ascertained by the judiciary on the basis of adequate provisions in the Law, in line with international human rights law and media freedom standards.

73. ISPs should be encouraged to self regulate in a manner upholding freedom of speech and expression, including through the development of code of conducts and clear guidelines on reporting and taking down suspicious websites/ online materials, while ensuring transparency and effective appeals procedures.

74. Because cyberspace transcends national borders, international co-operation on different levels is necessary to ensure that good practices are implemented in all jurisdictions and no safe haven is left from where terrorists can abuse the Internet.

75. All public and private stakeholders engaged in countering radicalization on the ideological level should leverage information and communication technologies – in particular the Internet – to challenge terrorist narratives, spread positive counter messages, and reach out to vulnerable groups as well as society at large.

76. Communication is key to mitigating the spread of violent extremist ideas, radicalization that leads to terrorism as well as the psychological impact of terrorism. Communication should always be backed by concrete actions.

77. State authorities and the Media should proactively engage with each other through regular interaction to develop contacts and a constructive relationship over time, before a crisis happens.

78. State authorities and Media stakeholders should reach a common understanding of the role(s) played by the Media in society, its functions, responsibilities and interests. This is a prerequisite to identifying opportunities and setting parameters for co-operation based on safeguarding the freedom and independence of the Media.

79. State authorities should be willing and organized to provide the Media with adequate information, to avoid situations where the Media can only turn to alternative, informal, sometime unreliable sources. The provision of information should not be manipulative and state authorities should timely speak out in reaction to instances of dis/misinformation. The Media themselves should timely react to such instances by making use of self-regulatory systems.

80. In the face of violent extremism and terrorism, the Media should be encouraged, including through self-regulatory mechanisms, to promote tolerance, non violence, social cohesion, and to facilitate the expression and public discussion of relevant issues/grievances. The Media should be encouraged to provide analytical reporting on terrorism rather than only descriptive and sometime sensationalistic coverage.

81. Self-regulatory initiatives by the Media should include guidelines on covering terrorism. Good practices should be promoted across borders.

82. State authorities should engage with the Media and support initiatives, in particular self-regulatory initiatives, with the aim of increasing Media stakeholders' understanding of violent extremism and terrorism, including factors conducive to terrorism, risk of manipulation of the Media by terrorists, nature of the terrorist threat, and the positive role the Media can play in countering the threat.

83. As part of preparedness and contingency planning in the event of a terrorist crisis, state authorities should be equipped and ready (structures and skills) to effectively and timely communicate with the public, through the Media, to prevent speculation, disinformation, and panic which might otherwise hamper response efforts and result in unnecessary damage/victims.