Organization for Security and Co-operation in Europe

Terrorist Use of the Internet: Threat, Issues, and Options for International Co-operation

Remarks by

Raphael F. Perl − Head of the OSCE Action against Terrorism Unit*

Before the

Second International Forum on Information Security

Garmisch-Partenkirchen, 7-10 April 2008

Ladies and Gentlemen, dear Colleagues,

First of all, I would like to say how pleased I am to be addressing this forum today. I thank the organizers very much for this opportunity to speak to you on this important and timely topic, and I wish them every success in their future work.

The Internet offers many advantages to legitimate users and to those who seek to use it for criminal purposes as well. It offers instant and almost secure communications worldwide. It offers a platform for the free dissemination and sharing of information across borders. It offers innovative and adaptable solutions to a plethora of activities.

The sophistication, speed, virtuality, and the relative anonymity that characterize the Internet and computer technologies are a major challenge to law enforcement. Investigating cases of Internet misuse by criminals and terrorists is time-consuming and time-sensitive. Law enforcement agencies very often lack adequate training and equipment. There are cumbersome problems in retrieving and securing electronic evidence. There are problems in presenting and simplifying this evidence for use in a trial.

My remarks will be divided into four parts. First, I will address the problem − the use of the Internet for terrorist purposes and the threat of cyber terrorism. Second, I will address the issue of obstacles to international legal co-operation in combating terrorism related computer crimes. Third, I will speak about the role of the International Community: what more could be done to combat the use of the Internet for terrorist purposes and to counter the threat of cyber terrorism. Fourth, I will briefly share with you what the Organization for Security and Co-operation in Europe (OSCE) has been doing to address the use of the Internet for terrorist purposes.

Terrorist use of the Internet and the threat of cyber terrorism

When we look at the world today, we see a world that is increasingly linked together and interdependent. It is linked together through economies – through trade. It is linked together through communications – through the Internet. The past decades have been marked by revolutionary progress in the area of information exchange and communication and I am sure that more innovations in the field of computer and Internet-based technologies are to come. This clearly presents us with invaluable opportunities. But it also poses challenges – many challenges today and probably new ones tomorrow.

* These remarks were prepared with the assistance and substantive input of Mr. Mehdi Knani

Coming from a Unit primarily concerned with terrorism, I will focus my remarks on the terrorist uses of the Internet and the threat of cyber terrorism. But this is not to downplay the importance of combating cyber criminality at large. On the contrary, much of what is and what *can be* done to combat the criminal use of the Internet and computer technologies can also serve counter-terrorism objectives.

I strongly believe that terrorism, regardless of its origin or purpose, if left unchecked for long enough, becomes a process, with vested interests in continuing that process. There are supply chains, salaries paid, fundraising efforts, training camps, recruitment, advertising and marketing, community services, indoctrination and many other activities. Many facilitators to this process exist: operational; logistical; ideological. Clearly, one very significant challenge relates to the Internet. The Internet and other modern computer technologies are central facilitators of terrorism as a process.

Terrorist use of the Internet

It will surprise no one that the Internet has become a strategic tool for terrorists and their violent extremist supporters. It is well known that Al Qaeda has been specifically recruiting persons with a computer sciences background and has been training its operatives in computer sciences. The use of the Internet by other terrorist groups such as the ETA is also extensively documented. The Internet represents a formidable tool for inciting to terrorism, recruiting, raising fund and potentially also conducting attacks on networked infrastructures.

The Internet today serves all. It is user blind. Hence the Internet is today one of the principal means whereby terrorist organizations disseminate propaganda, indoctrinate followers, recruit and train new operatives. There are websites regularly visited by tens of thousands of persons where prominent terrorist literature is made available and terrorist acts glorified. There are websites through which “leaders” interact directly with their supporters, creating social bonds and maintaining virtual communities, all of which can be later exploited to mobilize support. There are websites hosting virtual training camps as well as online manuals on how to assemble an explosive belt for instance or to create an explosive with every day life materials.

The Internet is also one of the principal means by which terrorists can raise and transfer funds and other material resources. Many of the emerging creative forms of terrorist financing are using the Internet.

The Internet also allows for instant and almost secure communication among terrorist operatives and between terrorist cells, including for the planning of attacks. In the past, only States enjoyed the advantage of such level of sophistication.

The threat of cyber terrorism

Moreover, the threat of cyber terrorism is very real, even though there has been – thus far – little evidence of active use of the Internet by terrorists to attack critical infrastructures. Hackers have repeatedly demonstrated their ability to violate the cyber integrity of some of the most secure systems, such as the one of the Pentagon. Recently also, Estonia has experienced the disruptive impact of cyber attacks. Similar attacks could have been launched with terrorist intent.

Cyber terrorism has a significant disruption potential in today’s world where most, if not all critical infrastructures are networked and connected to the outside via computer networks. The intentional spread of cyber viruses could lead to the breakdown or paralysis of entire critical systems, such as air traffic control or energy production plants, with potentially dramatic human costs. A particularly worrying threat is the potential conjunction of cyber attacks with traditional physical attack(s), or the launching of a cyber attack in times of major natural disaster crisis.

But cyber terrorism could also aim at inflicting economic costs, at times where communications and information exchange is essential to the functioning of our societies and to the global economic system. A central goal of Al-Qaeda inspired terrorists is to cause economic damage, not only physical damage. Increasingly therefore, I am convinced that communication networks are likely to become the target of terrorist cyber attacks seeking to paralyze our societies and economies.

One of the activities of my Unit, the OSCE Action against Terrorism Unit, is to raise awareness of the threat posed by the use of the Internet for terrorist purposes and to promote concerted efforts within the OSCE region and beyond to counter this threat. In the OSCE, we have been focusing in particular on the use of the Internet by terrorists for incitement purposes. I would like to share with you the following observations which derive from our work in this field, but also from promoting the international legal framework against terrorism and legal co-operation in criminal matters related to terrorism.

Obstacles to international co-operation in countering the use of Internet for terrorist purposes

Given the interconnectedness of national networks into a single worldwide web, international co-operation is an imperative to counter the use of the Internet for terrorist purposes. Sadly, many obstacles exist to effective international co-operation in general, and especially in this particular field. Terrorists and cyber criminals take advantage of these obstacles to escape justice and to pursue their activities with impunity.

The disparity of legal environments and practices

Importantly, different countries have different laws. The definition of crimes and sentences varies across jurisdictions. Different rules of evidence and standards of proof apply in one country than in another. There are often different procedural and evidentiary requirements for mutual assistance and extradition requests in different legal systems. Absence of relevant bilateral agreements and insufficient implementation of existing multilateral instruments to provide the necessary legal basis for judicial co-operation can also pose problems. Judicial officials may not be adequately trained in issues of legal co-operation in criminal matters. Language barriers and bureaucratic hurdles further complicate and slow down attempts to co-operate.

This regrettable situation is particularly acute in the case of the Internet and the regulation of on-line content and Internet-facilitated activities. There is a diversity of national laws applicable in this field, which may be specific to the Internet but are often not.

In dealing with the challenge posed by terrorist use of the Internet for incitement purposes, it is essential to distinguish between “illegal” and “objectionable” content. Regretfully however, universal agreement is lacking on what exactly constitutes “illegal” or “objectionable” content. Some countries have specific laws on incitement to and apology of terrorism. Some other countries rely on hate speech laws or other pieces of legislation. In the United States for instance, while there is no anti incitement statute *per se* in the law, there are a number of concepts which can be applied instead such as e.g. “criminal conspiracy” as well as “aiding and abetting” laws in order to prosecute in cases of terrorist use of the internet.

National legislations frequently differ in terms of the balance they strike with regard to freedom of expression when defining unlawful speech or content, including what is posted on the Internet. They also vary in terms of the degrees of explicitness, intent, and causality required for qualifying an act as incitement to terrorism or to another form of violence. For example, in the United Kingdom a new offence was introduced into the 2006 Terrorism Act which specifically outlaws the encouragement and glorification of terrorism. This offence covers the encouragement not of specific acts but of terrorism in general, and includes intentional and reckless statements, as well as publications. In Spain, the penal code defines incitement as *apologie*: the act of performing public ennoblement, praise and/or justification of a terrorist group, operative or act, regardless of how long ago it took place.

National legislations also differ in the extent Internet Service Providers (ISPs) can be liable for hosting illegal content and can be forced to retain/provide data. In fact, there is no universal agreement on exactly what role ISPs should play in combating cyber crime and cyber terrorism. Defining this role and the related responsibilities is a crucial task for the International Community in the future.

Further, national legislations differ in the balance they strike between privacy and data protection on the one hand, and, on the other hand, the needs of law-enforcement authorities in tracking suspected cyber-criminals and trying to collect evidence. In Germany for instance, the Federal Supreme Court recently ruled against the use of "Trojan" surveillance software by law-enforcement agencies without a warrant. This also links to the issue of anonymity on the Internet and the different options considered by countries to limit this anonymity. In Italy for instance, cyber cafés are required by law to ask for and register their customers' identity.

The need for international agreements

Thanks to the Internet information can freely circulate across borders and online activities are disconnected from a particular physical locale. Given the multiple jurisdictions likely to be therefore involved in Internet related criminal cases, international agreements promoting legal harmonization and standardized practice are indispensable. International agreements are indispensable to define the modalities for effective international co-operation. Otherwise, the discrepancies between national legislations allow for "venue-shopping" by ill-intentioned Internet users, who choose to post their unlawful material online, and/or to conduct their criminal activities, under the jurisdiction of states having the least restrictive, or no regulation, and thus enjoy virtual immunity. Terrorists can cross borders in cyber space at will. The law needs to be able to do the same. Important also is the issue of conducting investigations in multiple jurisdictions. How does law-enforcement accomplish this? Who should be in charge?

Speaking about international agreements and terrorism, I should of course also raise the issue of a universal definition of terrorism, which is often controversial. Defining terrorism is therefore an essential point of contention in the negotiation of a comprehensive universal convention against terrorism. What if an organization is considered as terrorist by country A, whereas it is considered as a legitimate national liberation movement by country B? Does terrorism necessitate *sine qua non* the intent to cause death or bodily injuries? Or can we consider cyber attacks aimed only at inflicting severe economic damage and disruption to be a form of cyber *terrorism*?

There is fortunately some room for co-operation without a universal definition of terrorism, by focusing on specific criminal offences related to a terrorist act. Arguably however, agreement on a material definition of terrorism and a comprehensive convention would facilitate and increase international co-operation against terrorism, including against terrorist use of the Internet. Nevertheless, terrorism always involves some form of criminal activity. This is where we all agree, and on this we should build to move forward.

The issue of law enforcement capabilities worldwide

Another obstacle to international co-operation in combating terrorist use of the Internet that I would like to highlight is the issue of capabilities. Appropriate national legislation and international co-operation agreements are indispensable but not enough. The technological and forensic capabilities of law enforcement agencies have to be commensurate to the challenges posed by the use of the Internet for terrorist purposes and other cyber criminal activities.

Terrorist uses of the Internet and cyber attacks are highly sophisticated, innovative and thus constantly evolving forms of crimes. Criminal computer programmes ("crimeware") are becoming increasingly difficult to detect. Cyber attacks are becoming increasingly more complex. Dynamic content on websites are increasingly difficult to trace (content of a given webpage coming from multiple locations that change from one moment to the next).This sophistication goes in conjunction with an increasing specialization of cyber criminals themselves.

The speed and immateriality that characterize computer activities and cyber communication further complicate attempts to monitor and to investigate cyber criminal activities. Countries have to work to enhance their law enforcement capabilities and keep abreast of the adaptability demonstrated by terrorists and other criminals in using the Internet and computer technologies. Importantly also, given the multiplicity of national jurisdictions potentially involved, *all* countries should build up such capabilities. Asymmetrical capabilities among countries will only impede the effectiveness of international co-operation in this field.

What could and should be done by the International Community

Strengthening the overarching international legal framework?

It is often said that the international legal framework against the use of the Internet for terrorist purposes should be strengthened. Some have called for a specific UN Security Council Resolution on combating the use of the Internet for terrorist purposes. Others have called for a specific international convention in this field under the auspices of the United Nations. Yet others favour the status quo, arguing that the issue is to implement the existing legal framework and to co-operate more effectively.

In the meantime we should not let the absence of a specific universal instrument impede international co-operation. The Council of Europe Convention on Cyber Crime (2001) has been recommended by many organizations, including the OSCE and Interpol, as providing an important international legal and procedural standard for fighting cyber crime. This Convention, in conjunction with other instruments, such as the Council of Europe Convention on the Prevention of Terrorism (2005), can provide sufficient legal basis for co-operation against the use of the Internet for terrorist purposes.

Strengthening international legal co-operation in criminal matters related to terrorism

Besides, more needs to be done by the International Community to facilitate and enhance international legal co-operation on criminal matters related to terrorism, such as financing, facilitation and preparation of attacks, or incitement to commit attacks, irrespective of their commission through computer technologies and the Internet. There is an array of international instruments already applicable to these offences. In particular, we need to continue promoting the ratification and implementation of the universal counter terrorism conventions and protocols as well as the UN convention against transnational organized crime and its protocols. We should also continue promoting the implementation of the relevant United Nations Security Council Resolutions, especially resolutions 1373 (2001) and 1566 (2004) which require States to fully co-operate in the fight against terrorism, as well as resolution1624 (2005) which calls upon States to "prohibit by law incitement to commit a terrorist act or acts". On the regional level as well, the most should be made of existing instruments such as the different Council of Europe (CoE) conventions on terrorism. All these multilateral instruments contain valuable provisions for co-operation on terrorism related offences, possibly carried out via the Internet.

Important also to international co-operation in criminal matters related to terrorism is the continued promotion and utilization of the wide range of technical assistance tools developed by the United Nations Office on Drugs and Crime (UNODC), including model laws and treaties on mutual legal assistance and extradition, legislative guides for the implementation of international conventions in national law. The UNODC has also developed a very practical *Mutual Legal Assistance Request Writer Tool*, already available in English, French, Spanish, soon in Russian and Portuguese and somewhat later in Chinese and Arabic. Similar software for writing extradition requests is expected to be finalized this year.

Training of judicial officials is an essential component of effective international co-operation on criminal matters related to terrorism. Sadly, what has been done in this respect remains insufficient. Additional efforts are needed to train prosecutors, judges and other officials on issues of international legal co-operation in criminal matters, including computer and Internet facilitated crimes. The international community should develop and focus on "train-the-trainers" capacity building programmes in order to enhance the impact of its work and achieve better results.

Promoting the exchange of information and good practices

There is also a need to further promote the exchange of information and good practices between countries on preventing cyber terrorism and countering the use of the Internet for terrorist purposes. Countries can learn from each other in terms of legislative amendments, procedures and mechanisms adopted, for instance, to criminalize incitement, to quickly collect and secure electronic evidence, to shut down in an expeditious but human rights compliant manner websites that support terrorists.

I should mention here the example of the G8 High Tech Crime Sub Group, and its work on preventing, investigating, and prosecuting crimes involving computers and networked communications, including terrorist uses of the Internet. The Group has elaborated various best practices documents, guides, as well as assessments of threats to and impact on law enforcement from new technologies (e.g. wireless, encryption, viruses and other malicious programmes).

Strengthening law enforcement forensic capabilities worldwide

More needs to be done also in terms of strengthening national forensic capabilities to enable law enforcement agencies to act quickly against terrorist abuse of the Internet and / or to protect vital information infrastructures from cyber attacks. Just like it takes a thief to catch a thief, it takes a computer specialist to catch a cyber-criminal. The United States for instance has established in 2003 a Computer Emergency Readiness Team (CERT) to protect the country's Internet Infrastructure. International support should increasingly be provided to countries with limited resources to assist them in setting up specialized units, with the adequate training, equipment and other resources, to deal with cyber crime, terrorist uses of the Internet and cyber terrorism.

Noteworthy here is the work of Interpol. Interpol already provides a specialized training known as Training and Operational Standards Initiative for High Tech Crime (TOPSI), which is aimed specifically at cyber crime and includes a train-the-trainer component. But in the words of Interpol's Secretary General, if we are honest and look at the risks before us worldwide and the need for training, these efforts need to be raised 100, if not 1000 times to keep pace with the cyber-criminal threat.

Promoting speedy information exchange and intelligence sharing on a day-to-day basis

Speedy information exchange and intelligence sharing on a day-to-day basis on the use of the Internet for terrorist purposes should be encouraged and intensified as much as possible. The G8 Computer Crime Network has already proven to be a very effective mechanism of co-operation in investigating cyber crimes. A related positive development is the fact that there are now efforts to consolidate the G8 and the Council of Europe lists of contact points into a comprehensive one. Interpol has also been urging countries to establish National Central Reference Points (NCRPs) on cyber crime to be part of a network using its secure police communications system. This would enable police anywhere in the world to immediately identify and obtain assistance from cyber crime experts in other countries 24 hours a day.

Effectively monitoring the Internet and exploiting relevant online material

Effectively monitoring the Internet has also been an issue. Due to insufficient resources, much of the counter-terrorism relevant material on the Internet remains unexploited. Likewise, language barriers are a significant impediment to the effective monitoring of the online presence and activities of terrorist groups. It seems therefore realistic and potentially beneficial for countries to pool resources into joint monitoring of the Internet. This has already been taking place at the national level in some countries such as Germany, where an inter-agency *Joint Internet Centre* was established in January 2007. Similar efforts have also been undertaken at the regional level and should be promoted further. The “Check the Web” initiative, for instance, is a law enforcement tool developed by Europol and aiming to facilitate the exchange of information on online Islamist terrorist propaganda material. It consists in an Internet based library available exclusively via the Europol Virtual Private Network (VPN), which offers a restricted access to selected law enforcement officials from all EU Member States.

Promoting models for advanced co-operation in criminal matters

Many models for advanced co-operation in criminal matters exist and could be applied to cases of terrorist use of the Internet. For example, some countries have established liaison offices abroad which are staffed with intelligence officials and/or magistrates (e.g. FBI and US Department of Justice overseas liaison representatives). We could imagine that some of these officials be trained on, or be complemented by experts on cyber crime and terrorist use of the Internet. In addition other countries have set up joint investigative teams for comprehensive co-operation on connected cases (e.g. Spain and France on ETA). We could imagine that joint investigative teams be created to address specific cases of terrorist use of the Internet.

Promoting public private partnerships

The last point I would like to raise, in terms of what more could be done by the International Community, is the promotion of public private partnerships (PPPs) with the industry and civil society to counter the use of the Internet for terrorist purposes. The importance of PPPs in this regard cannot be overstated. The Russian Federation and the United States have put PPPs in the forefront of the OSCE counter-terrorism agenda.

The Internet is in the private sector; key service providers are found in the industry not in government. And the business community has suffered from cyber-attacks for some time now. The private sector therefore is our most natural ally in combating the use of Internet for terrorist purposes. It is of crucial importance to establish the necessary trust and relationships, as well as to identify and disseminate best practices.

More needs to be done to identify and disseminate successful models for PPPs with the industry to secure communication networks and computer facilities against cyber attacks.

More needs to be done with regards to PPPs to encourage self-regulatory approaches by the Internet community to online activities and material. The private sector can be involved both as an alternative to potentially too restrictive public regulation, and in support to law-enforcement – in terms of monitoring for instance.

More needs to be done also for the development of an active, educated and vigilant civil society, which is essential for effective counter-terrorism measures regarding the cyberspace. Internet users should be aware of the intrinsic risks of the Internet, including the possible misuse of information that they make available online.

The OSCE contribution to countering the use of the Internet for terrorist purposes

My Unit, the OSCE Action against Terrorism Unit (ATU) has been engaged on different fronts directly or indirectly relevant to countering the use of the Internet for terrorist purposes. It is not practical here to go into the details of our activities but let me give you a brief overview.

Political Framework for OSCE action against the use of the Internet for terrorist purposes

Concerned by the extent of the use of the Internet by terrorist organizations, OSCE participating States have adopted two ministerial decisions (MC.DEC No. 3/04 and MC.DEC No. 7/06), the first one in 2004 and a subsequent one in 2006. These decisions serve as the basis for the OSCE's activities in this area.

Within the framework of these decisions, the OSCE promotes international co-operation on countering the use of the Internet for terrorist purposes, and promotes the exchange of relevant information. We also promote participation in the G8 24/7 Computer Crime Network, as well as exploration of possibilities for more active engagement of civil society institutions and the private sector. We do this notably by promoting public-private partnerships in preventing and countering the use of the Internet for terrorist purposes. We also promote the relevant work done by the Council of Europe.

OSCE expert workshops on the use of the Internet for terrorist purposes

In implementation of the aforementioned decisions, the ATU has already organized three action-oriented OSCE-wide expert workshops:

- an *OSCE Expert Workshop on Combating the Use of the Internet for Terrorist Purposes* held in Vienna in October 2005;
- a joint *OSCE/Council of Europe Expert Workshop on Preventing Terrorism: Fighting Incitement and Related Terrorist Activities*, held in October 2006 and which dedicated an entire session to the topic;
- and our most recent event, namely the *2007 Expert Workshop on Combating Incitement to Terrorism on the Internet,* represented the logical and necessary continuation and fusion of previous ATU efforts in the inter-linked thematic areas of combating the use of the Internet for terrorist purposes and in the area of fighting incitement to terrorism and related terrorist activities.

Taken together, our three workshops have brought together almost 500 participants from more than 50 countries, including more than 20 of the world's foremost experts on the subject, as well as policy makers and stakeholders from the private sector. Our workshops have adopted a cross-dimensional and multifaceted approach taking into account a series of aspects which require sustained attention: threat assessment, disparity of legal environments and practices, identification and dissemination of best practices, improvement of the international co-operation in that field, human rights concerns and freedom of the media, use of the Internet to counter the spread of ideas endorsing terrorism.

Looking ahead, at the initiative of Estonia we are currently in the process of expanding our work on combating terrorist use of the Internet into the area of cyber security. These days, a food-for-thought paper, drafted with input from the ATU, is being presented to OSCE participating States. It calls for the organization of an event on the aforementioned topic.

Promotion of international legal co-operation in criminal matters related to terrorism

The ATU has also a strong record of activity in promoting international legal co-operation in criminal matters related to terrorist offences, some of which – such as terrorism financing – can have possibly been carried out through the Internet. Training is an important issue here, and we have organized in close co-operation with UNODC, three large scale OSCE-wide workshops in Vienna, three sub-regional workshops, and three national training workshops. All in all, more than 870 legal practitioners (prosecutors, judges) and other officials from 64 OSCE participating States and Partners for Co-operation have attended these OSCE workshops, discussing the universal and European legal framework for mutual legal assistance and extradition, relevant human rights aspects, practical issues, challenges and possible solutions in legal co-operation in criminal matters related to terrorism.

Relevant activities of other OSCE bodies

There are other institutions within the OSCE doing relevant work on issues pertaining to the Internet. Our colleagues from the Office of the Co-ordinator of Economic and Environmental Activities (OCEEA), for example, are active in the area of cyber crime, in particular as it pertains to money laundering and combating the financing of terrorism. Similarly, our colleagues at the OSCE's Strategic Police Matters Unit (SPMU) have looked into combating child-pornography online. In addition, the OSCE Office in Yerevan initiated the establishment of a Cyber Security task Force (CTF) in Armenia which prepared a publication outlining the main aspects of cyber-security in the Republic of Armenia.

Furthermore, at the ATU events I previously mentioned the OSCE's Office for Democratic Institutions and Human Rights (ODIHR) as well as the Representative on Freedom of the Media (RFoM) co-operated with us and presented their views on the subject. This was to ensure that the relevant human rights and civil liberties considerations are duly taken into account.

In particular, I would like to refer you to the work of the OSCE Representative on the Freedom of the Media, and its publications "Governing the Internet" of 2007 and "Media Freedom Internet Cookbook" of 2004. Both publications are available online.

Concluding observations

I would like to conclude now by emphasizing a few thoughts. The process of globalization offers many opportunities and advantages to mankind. Inherent in this process is the facilitation and free movements of people, goods, services, money and information, in a relatively open and unregulated environment.

The flip side of globalization is that such conditions provide the same advantages for illicit criminal activities. Effective international co-operation is thus essential to address this challenge. The Internet could not be more representative of this somehow paradoxical situation where new opportunities create increasing challenges and acute need for international co-operation.

Terrorist use of the Internet is one of these challenges and it is clearly on the rise. Contemporary terrorism has become a virtual movement with the Internet being the cement holding it together. Terrorist groups are well aware of the significance of the Internet to their cause. It is one of the key "facilitators" of the process of terrorism. Terrorism tends to increasingly become a virtual movement using the cyberspace as a strategic battleground.

In dealing with the challenge posed by terrorist use of the Internet, one of the key issues is to distinguish between "illegal" and "objectionable" content. Problematically however, there is no universal agreement on what exactly constitutes such content. Combating terrorist incitement on the Internet requires the balancing of counter-terrorism measures with issues of free speech and the protection of civil liberties. States need to come to terms with the dual-responsibilities of ensuring freedoms for their citizens while also not shirking from taking the necessary steps to protect them from violence.

Office of the Secretary General
Action against Terrorism Unit
Wallnerstrasse 6, A - 1010 Vienna
Tel: +43(0)1 514 36 -6702   Fax: -6687
Mail: atu@osce.org
osce.org/atu