



**Organization for Security and Co-operation in Europe
Office of the Representative on Freedom of the Media**

**Position Paper by the Office of the Representative on Freedom of the Media to the
“OSCE Conference on a Comprehensive Approach to Cyber Security: Exploring the
Future OSCE Role”, 9-10 May 2011, Vienna.**

Success via cooperation

One of the outstanding features of the OSCE is the comprehensive multi-dimensional concept of security developed within the Helsinki process. The Astana Summit Declaration reaffirms these fundamental and supports and endorses the importance of human rights and fundamental freedoms in relation to Security matters

Cyberspace is challenging almost every aspect of traditional ways of regulating communications media. It is almost impossible to control many millions of one-to-one interactions and regarding the Internet as infrastructure and as a tool that can promote the realization of fundamental rights, including the right to free expression and media freedom, there are many new challenges to embrace.

This conference offers an opportunity to explore how the OSCE, with its comprehensive and multi-dimensional approach by involving all stakeholders, can contribute to the fight against cyber threats and at the same time ensure our shared values of human rights, fundamental freedoms and democracy remain firmly entrenched.

There is no effective and long-lasting security without the free flow of information and free expression. Freedom of expression and a free media play important roles in fostering meaningful debate on hard security matters. Free media can help us to effectively address new challenges.

Human rights including the freedom to express ourselves should not be seen as inflexible obstacles to effective intelligence, police and military action. In fact, those can only be achieved through free media, free expression and free debate.

Taking legal action against illegal material can be difficult, depending on where the material is physically placed, in order to avoid abuse and arbitrary application of laws. It should be ensured that illegal content must be prosecuted in the country of its origin and that all legislative and law enforcement activity must clearly target only illegal content and not the infrastructure of the Internet itself.

Terrorists, like other criminals, can use the Internet, like mainstream media or the public, for malicious purposes, including disseminating materials designed to encourage terrorist acts or establishing communications to plan and coordinate terrorist acts. Use of the Internet for these purposes has become more widespread. However, the advantages of the Internet as a tool for the exercise of human rights, including the right to free expression clearly outweigh existing negative features.

While no one questions the legitimate right of a government to function and to tackle the issue of cyber-security and cyber attacks, the Representative also realizes that governments often block “uncomfortable” websites and regulate the Internet using national security or the fight against terrorism as a pretext.

Governments have obligations under international laws and conventions, including OSCE commitments to protect freedom of expression, to consider when regulating the Internet.¹ The Representative believes that instead of considering free media a tool to assist terrorists in achieving their goals, it is an essential element to fighting the threat. Media, including the Internet, can help save lives by spreading information of public interest. It can show the true face of terrorism by engaging in investigative reporting. Media can raise awareness of the danger of terrorism and the efforts to combat it. Finally, it can counter the objective of terrorists – to destroy societies’ basic human rights, including the right of free expression.

The OSCE, with its multi-dimensional approach to security, cannot afford to ignore these issues. The Representative has drawn up a list of key principles that participating States and the OSCE should consider when combating the use of the Internet for terrorist purposes, in view of their obligations under international laws and conventions and OSCE commitments to protect freedom of expression and free media, including free expression on the Internet.

The key principles are aimed at avoiding over-regulation of the Internet, vague legal definitions and the potential abuse of laws under the pretext of fighting terrorism, but bearing the risk of curbing free speech and silencing free and critical media. These principles are based on the fact that free media itself is essential to fighting threats of terrorism as media can raise awareness of the danger of terrorism and the efforts to combat it.

Attempts to regulate the flow of information should be carefully considered:

- Measures undertaken by authorities should be directed only against illegal content.
- If a website must be closed, such action has to be based in law, should fall under the responsibility of courts of law and should not lie in the hands of private companies.

¹ OSCE Ministerial Council Decision 03/04 on Combating the Use of the Internet for Terrorist Purposes
OSCE Ministerial Council Decision 12/04 on Tolerance and Non-Discrimination
OSCE Permanent Council Decision No. 633 on Promoting Tolerance and Media Freedom on the Internet
OSCE Ministerial Council Decision 7/06 on Countering the Use of the Internet for Terrorist Purposes

- The procedures for closing a website should be transparent affected parties should have the right to appeal.
- Any restrictive measure taken should follow the principles of the “upload-rule,” meaning that the content of a website has to be in compliance with the laws of the country of its origin and not with those of the country where the content is downloaded.

Additionally, it needs to be noted that filtering and blocking websites is generally not in accord with OSCE principles. In fact, people should decide for themselves which websites they wish to access.

Beginning in 2004, the Representative has contributed to several OSCE events regarding hate speech on the Internet. The Representative has made it clear that an educated mind is the best "filter" imaginable. The Office published the “Media Freedom Internet Cookbook” a study on “Internet Governance in the OSCE Region,” and “The Media Self-Regulation Guidebook,” which serve as further resources.

It should be emphasized that the Internet also offers opportunities for promoting tolerance and fostering mutual understanding. These positive features should be taken into account when fighting illegal content.

Concerned about the proliferation of anti-terrorism laws, four international rapporteurs on freedom of expression² adopted on 9 December 2008 a “Joint Declaration on Defamation of Religions, and Anti-Terrorism and Anti-Extremism Legislation” stating that the definition of terrorism “should be restricted to violent crimes that are designed to advance an ideological, religious, political or organised criminal cause and to influence public authorities by inflicting terror on the public”.³ The four rapporteurs cautioned against States employing vague terms such as “glorifying” or “promoting” terrorism or extremism. In their 2005 Joint Declaration on the Internet and Anti-Terrorism Measures, the rapporteurs stress that “incitement should be understood as a direct call to engage in terrorism, with the intention that this should promote terrorism, and in a context in which the call is directly causally responsible for increasing the actual likelihood of a terrorist act occurring.”⁴

Over the last few years many OSCE participating States have embarked on regulating online free expression and Internet-based media. In addition, legislative provisions aimed at transnational threats, cyber crime and hate speech on the Internet have been passed or amended. Online journalists and online media are facing mounting difficulties when performing their duties. Also, the regulation of the multi-layered online medium has led to challenging restrictions to the free flow of information on the Internet.

² The UN Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of the Media, the OAS Special Rapporteur on Freedom of Expression and the Special Rapporteur on Freedom of Expression and Access to Information of the African Commission on Human and Peoples’ Rights.

³ http://www.osce.org/documents/rfm/2008/12/35705_en.pdf

See also the Amsterdam Recommendations of 14 June 2003 on Freedom of the Media and the Internet of the Office of the Representative on Freedom of the Media at <http://www.osce.org/fom/41903>

⁴ Joint Declaration of 21 December 2005 at <http://www.osce.org/fom/27455>

In 2010 the Representative therefore developed a comprehensive survey to assess the extent of Internet regulation across the OSCE region. The ongoing study is looking into existing legislation and practices related to the free flow of information and freedom of expression on the Internet. The purpose is to prepare an overview of legislative provisions and governmental practices and to assess the impact of these laws and practices on media freedom and media pluralism on the Internet.

A final report is due later this year. The Representative already shared the model of this survey with other international organizations seeking similar data.

All actors should be thinking in terms of a new synthesis of specific and comprehensive ways to create a real and effective way to fight terrorism in cyberspace while at the same time protecting human rights, including the right to free expression and free media.

The best way to start is by engaging all the structures of the OSCE, including its Institutions, field operations and the Secretariat, because only close co-operation will provide the crucial blueprint for bringing together all aspects of the of the matrix necessary for a successful strategy.