CoE – OAS/CICTE Conference on Terrorism and Cyber Security

CONCLUSIONS

San Lorenzo de El Escorial, Madrid, Spain, April 16-17, 2009

This International Conference on Terrorism and Cyber Security was organised jointly by the Council of Europe and OAS/CICTE, and marks the first joint trans-regional event of its kind focused on these issues. This conference has been organised under the Spanish Chairmanship in the Council of Europe Committee of Ministers, and participants acknowledge and appreciate the substantive contribution of Spanish authorities to the success of this event.

Those taking part included experts from the CoE and OAS member and observer States, as well as several international organisations, the private sector and academia.

The discussions ended with the reading out, on behalf of the Council of Europe and OAS/CICTE Secretariats, of the following conclusions:

While the conference focused on ways in which the Internet is misused by terrorist organisations and their supporters – and the numerous risks that this poses – it was underlined that the Internet has proven an overwhelmingly beneficial development for modern society precisely for the way in which it has revolutionized the dissemination of ideas and information, and the formation of networks.

Yet the scope and transnational nature of the Internet, and the fact that it is largely user-controlled, can present a challenge to national governments when these ideas, information or networks are intended to or have the effect of undermining national or regional security, the rule of law, or respect for human rights and democracy.

The use of the Internet by terrorists as a tool for supporting or perpetrating their activities, and the potential for cyber-attacks by terrorists against critical infrastructure, are among the primary challenges countries may face in terms of the misuse of the Internet, and increasingly cannot be separated from terrorist activities otherwise.

Regarding **The Internet as a tool to support terrorism,** discussion focused on terrorist organisations' presence on and use of the Internet for various purposes, including the dissemination of propaganda related to ideology and activities, and as a means of promoting radicalization within target communities. It was noted that terrorist groups are able to use the Internet for recruitment and training purposes, as well as a tool for all aspects of financing terrorist activities. Terrorist groups and their supporters have taken advantage of the anonymity and wide reach of the Internet to exploit it for these purposes, a fact which has complicated governments' ability to track and stop terrorist activities on-line.

To confront these challenges experts are proposing a range of innovative solutions that go beyond purely technical ones. Among these, *inter alia*, are deterring the production of extremist materials, promoting self-regulation of on-line communities and seeking to advance a positive counter-narrative to extremist messages. It was suggested that policy-makers and law enforcement should take into account these elements while developing a strategy for prosecuting cases regarding terrorist use of the internet.

Regarding **Countering the use of the Internet by terrorists**, a case study illustrated the numerous challenges for law enforcement and prosecutors in investigating and prosecuting terrorists' use of the Internet. Given the transnational nature of terrorists' activities on-line, and the volume and technical sophistication of the evidence that can be collected, the investigation and prosecution of these cases are often highly complex and require active cooperation between investigators and prosecutors, both at the national and international levels.

At the international level it was noted that a transnational legal strategy might benefit the efforts of law enforcement and other government authorities to counter the use of the Internet by terrorists. Particular attention should be paid to enhancing the efficiency and rapidity of cooperation between appropriate authorities and other stakeholders. A number of suggestions were put forth in this regard, including: the active use of existing tools, networks, and relevant legal instruments for international cooperation; enhanced early dialogue among counterparts in distinct jurisdictions; and more active involvement of technical experts.

In addition, it was stated that engagement with the private sector is key to denying terrorist groups the platform for disseminating their radical message and inciting violence. The role of civil society was also discussed as a potentially powerful force for diminishing the audience and support for – and presenting a counter-narrative to – terrorist organisations and their supporters' efforts to promote radicalization and recruit support on-line.

A discussion of **The potential for cyber attacks by terrorists** noted that while terrorist organisations appear to be motivated to launch cyber attacks against their enemies, at the present time their ability to affect large-scale disruption or destruction via cyber means appears to be limited. While the capabilities of such organisations to perpetrate cyber attacks are likely to increase in the future, the extent to which these will cause sustained mass disruption or destruction is less certain. A more immediate threat is that of a cyber attack combined with a physical attack, for example on physical critical infrastructure such as a nuclear or other energy facility. Such an attack could prove particularly difficult to confront, and could potentially have a devastating impact.

Assessing risk and vulnerability is critical in order to determine whether in fact critical information infrastructure is protected, and what the potential impact of an attack on such infrastructure would be. The international community should prepare for the growing cyber capabilities of terrorists in addition to the threats posed by cyber criminals and other such actors. While protective measures are essential in this regard, additional emphasis should be placed on developing the capabilities and mechanisms to ensure resilience in the face of an attack.

This led to a discussion of **Protecting critical infrastructure and developing the capability to defend against and respond to cyber attacks by terrorists**, which highlighted some of the key areas where governments and private sector stakeholders should focus their efforts. It has been recommended that States should establish and develop a national Computer Security Incident Response Team (CSIRTs), to serve as a focal point for the exchange of information regarding cyber incidents affecting critical information infrastructure, and to coordinate incident response and mitigation among affected stakeholders. Given the fact that private sector entities comprise a majority of stakeholders in the area of critical infrastructure, ensuring resilience in the face of cyber attacks is fundamental, and requires an enhanced partnership between the public and private sectors. Furthermore, the transnational nature of cyber threats requires that

there be effective regional and international networks to promote cooperation and information-sharing among these national CSIRTs.

In light of all of the aforementioned, the final discussion focused on the need to develop a national cyber security strategy as a basis for coordinating national efforts in the areas of legislation, law enforcement, engagement of civil society and the private sector, and developing the capabilities for watch, warning and incident response.

A comprehensive national, regional and trans-regional approach to cyber security aimed at deterring terrorists´ use of the internet and the protection of critical infrastructure from cyber and other attacks by terrorists is vital to ensuring the security of States and their citizens, and preserving stability, the rule of law, and the full protection of fundamental rights and freedoms.

To conclude, the organizers and the participants acknowledge that this conference highlights the need to step up national efforts as well as bilateral, subregional, regional and international cooperation, to counter terrorism in general, and specifically where it converges with our increasing use and benefit of the Internet and other critical information infrastructure.

These national and regional efforts should be carried out in line with the UN Global Counter-terrorism Strategy, and in cooperation with the relevant UN entities.