23/11/2016

Speech

By

Jan Kleijssen

Director

Information Society and Action against Crime Directorate

Directorate General Human Rights and Rule of Law – DGI

Council of Europe

Special Meeting of the Counter-Terrorism Committee with Member States and relevant international and regional organisations, civil society and the private sector on

"Preventing the Exploitation of Information and Communications Technologies for Terrorist Purposes, while Respecting Human Rights and Fundamental Freedoms"

New York, 1 December 2016

Pasted below are a number of questions you may wish to consider for your presentations:

- *What are the main political, legal, and administrative **challenges to the improvement of mutual legal assistance in electronic matters**?*
- *What **regional and bilateral good practices** have you identified should be promoted at the **global level**?*
- *Given the difficulties of changing the current international framework of cooperation, what **practical measures could be taken** to improve the current system?*
- *What measures could be taken to **improve** the **cooperation** between **law enforcement and the private actors**?*

*We ask that each speaker limit his or her presentation to **10 minutes** in order to allow sufficient time for Q and As.*

Excellences, dear colleagues,

The Council of Europe is pleased to be able to work alongside the United Nations, among other organisations present here today, to help address the many issues raised by the exploitation of information and communications technologies by terrorists and their supporters.

Since 1960, the Council of Europe has laid the foundations for co-operation in criminal matters between Council of Europe member states. The question we now ask is: after 60 years of efforts and work to strengthen relations between states, has international co-operation in criminal matters produced meaningful results?

But perhaps most importantly, how can we profit from these decades of experience to meet the real challenges of contemporary criminal justice?

To a large degree, the tools exist: The Council of Europe oversees the implementation of 14 Treaties on international co-operation in criminal matters, covering aspects of procedural and substantial criminal law, providing a number of useful mechanisms for mutual legal assistance, extradition, transfer of proceedings, transfer of prisoners, among other areas of co-operation.

The Conventions on criminal matters are widely ratified among the 47 member States, and are open for signature and ratification by other interested non-European States.

A good example of this is the European Convention on the Transfer of Sentenced Persons, ratified by over 65 States, or the Budapest Convention on Cybercrime, ratified by 50 States including Australia, Canada, Japan, Israel and the United States of America.

The Council works hard with member States to make sure that all instruments are efficient and well-adapted to the shifting international cooperation environment. As new challenges emerge, existing instruments are reviewed, kept up to date, and operational.

The question is whether to draw up new legal instruments or, instead, focus on improving those which already exist. It could be said that drafting new legal instruments would not resolve the difficulties encountered and would not produce better outcomes, but could further complicate the understanding of the various texts and thus produce the opposite effect.

It is therefore absolutely vital to strengthen the implementation of the existing instruments by all players involved in international co-operation in criminal matters. The Council of Europe aims to facilitate proper international cooperation in these areas, which is especially important in counter-terrorism activities where the consequences of failing to act effectively can be catastrophic.

Regardless, we must try to strike the delicate balance of ensuring that action against terrorist activity online requires certain safeguards to ensure compliance with applicable human rights law and rule of law standards. The European Convention of Human Rights and the European Court of Human Rights has long been a key institution in helping to shape and guide the law when it comes to criminal investigations and criminal proceedings.

The Court has dealt with many relevant aspects of terrorist activity relevant to today's topic, in particular in elaborating on human rights standards for fair trials, for example when it comes to rules of evidence and procedure.

The two most important instruments are the 2005 Convention on the Prevention of Terrorism and the recent 2015 Additional Protocol which addressed the foreign terrorist fighter phenomenon.

This latter instrument enabled the implementation of a 24/7 FTF Network, a real time police information exchange system operationalised prior to ratification of the Additional Protocol. The aim of the 24/7 Network is to ensure that border guards or other law enforcement agents confronted with suspicious travellers, potentially based on digital evidence, should be able to communicate with their counterparts immediately, through the designated contact points.

The Council of Europe also provides a number of practical tools to help states to effectively implement their obligations under the Conventions.

The best example I want to highlight here are the Council of Europe's model request forms and guidelines for mutual legal assistance (MLA) practitioners, both of which are available freely from our website. Such tools are important for the purposes of improving mutual legal assistance activities as they help avoid the submission of inaccurate or incomplete requests while also raising awareness among practitioners of the relevant Conventions that can be used

These tools are based on the guiding principles that *requested* States should treat requests with the same efficiency and promptness they would expect others to treat their own requests, and that *requesting* States should not focus on specific measures, but rather on the result they wish to achieve.

The MLA guidelines also include a chapter on requests for electronic data on the basis of the Budapest Convention. The Council of Europe has observed a trend whereby requests for information are conducted directly, where possible, without using traditional MLA request mechanisms.

As such, the Council of Europe is looking at the possibility of developing more appropriate tools for states seeking and requesting digital information. These tools could be developed to help private

internet companies, such as internet service providers, communications services and content-hosting platforms, to execute requests by law enforcement entities in a proper, expedited and effective manner.

These model information request forms will be based on similar general principles as the MLA model request forms, particularly that they will try to find uniform standards, facilitate operational engagement, and help avoid incomplete or unworkable requests.

It is clear that public/private cooperation is essential when it comes to the rule of law in cyberspace, be it in relation to terrorism, cybercrime or evidence in the cloud, and the Council of Europe aims to make life easier for both state institutions and private companies.

Within the framework of the Budapest Convention on Cybercrime which has been the leading treaty on “international cooperation in digital matters” as far as cybercrime and electronic evidence is concerned for 15 years, cooperation between law enforcement authorities of states, on the one hand, and private companies, on the other, has already been established.

Eight years ago, in April 2008, the Council of Europe developed a set of informal Guidelines on law enforcement/service provider cooperation on cybercrime. In December 2008, the European Court of Human Rights then referred to these Guidelines in its judgment on K.U. versus Finland and underlined the need for a culture of

cooperation between law enforcement and service providers so that governments can meet their obligation to protect individuals against crime.

Working groups of the Cybercrime Convention Committee held numerous meetings with service providers since then. In the future such meetings will take place on a regular basis. Furthermore, the Council of Europe will involve providers in capacity building activities.

In addition to the already existing public/private cooperation on cybercrime, the Council of Europe is currently in the process of establishing a platform between governments and major Internet companies and representative associations on their respect for human rights online, to protect, respect and remedy challenges and violations to them as called for in the recently adopted Council of Europe Internet Governance Strategy (2016 – 2019).

Under the aegis of this platform, the Council of Europe intends to broaden the public/private cooperation to cover also the abuse of the Internet for terrorist purposes in addition to the cooperation already undertaken in the framework of cybercrime. Possible topics to be discussed between governments and major Internet companies and representative associations include the facilitation of law enforcement cooperation on legal and/or technical aspects of filtering/removing terrorist content and taking down identified user accounts; guidelines on Internet companies' means and methods of identifying, tracking and/or filtering of online terrorist content; furthering counter-

narratives to terrorism through techniques such as context-based search engine indexing; and last, but not least, effective remedies to address illegitimate restrictions or infringements of human rights and fundamental freedoms online.

The Council of Europe is of course aware, that similar initiatives to combat terrorism online have recently been launched by, *inter alia*, the United Nations, at the global level, and the European Union, at the regional, European level. However, we consider that the added value of furthering public/private cooperation in this field based on our long-standing experience in the balancing of human rights and security needs, and at a pan-European level, is still significant. That said, coordination with other initiatives of a similar nature both, globally and regionally is a must.

Let me now revert to the Budapest Convention on Cybercrime.

About one third of all states are either Parties (50) or have signed it or been invited to accede (17) and another one third have used it as guideline for domestic legislation.

Recently, on 15 November 2016, the Cybercrime Convention Committee adopted a Guidance Note showing how the provisions of the Budapest Convention can be used to address aspects of terrorism.

This not only applies to substantive law, but also to procedural law and international cooperation.

The Budapest Convention requires parties to adopt a set of procedural powers to secure electronic evidence, such as search and seizure of computer systems, production orders for data, interception of communications etc. These are subject to rule of law safeguards. They apply to electronic evidence in relation to any crime, including in relation to terrorist offences. International cooperation provisions also largely apply to cooperation in cases of electronic evidence, not just cybercrime.

One difficulty that criminal justice authorities are faced with is that electronic evidence needed is increasingly in foreign, unknown, multiple or shifting jurisdictions.

Mutual legal assistance arrangements are thus not always feasible or too cumbersome to secure volatile electronic evidence.

The Cybercrime Convention Committee therefore established two years ago a Cloud Evidence Working Group to identify solutions.

The Recommendations of the Cloud Evidence Group were discussed by the Committee and by the international Octopus Conference from 14 to 18 November. The results are as follows:

There is full agreement that mutual legal assistance must be made more efficient when it comes to electronic evidence. This includes training and allocation of resources but also the establishment of emergency procedures, including for example in the case of terrorist threats.

There is broad support for, but not yet full consensus on, a Guidance Note on the Production of Subscriber Information. This Guidance Note – once adopted – would mean that criminal justice authorities would be able to request a service provider offering a service in the territory of a Party to produce subscriber information for example of a webmail or social media account even if the data or the provider are in another jurisdiction. This is already current practice but the legal basis has been unclear. If the Guidance Note stands, Article 18 Budapest Convention could serve as the domestic legal basis.

There is full support to a set of practical measures to enhance cooperation with multi-national service providers. This includes regular meetings of the Committee with service providers, or an online tool providing information to providers on the domestic legal basis when an authority in a Party orders the production of data, and conversely information on the policies of providers for criminal justice authorities.

There is broad support for the preparation of a Protocol the Budapest Convention covering additional possibilities for mutual legal assistance, conditions for direct trans-border access to data,

provisions for direct cooperation with providers in other jurisdictions and provisions for the protection of personal data.

The Cybercrime Convention Committee will hopefully decide in June 2017 whether to go ahead with the negotiation of a Protocol to the Budapest Convention.

These developments show that the Convention on Cybercrime is alive and kicking. It is able to address complex challenges, including in relation to the terrorist misuse of information technologies, while at the same time ensuring that rule of law requirements are met.

International co-operation to fight crime and terrorism matters must not be seen as an aim in itself, but as an indispensable means to address transnational problems effectively. The international community already has effective tools. They must now be put into effect.