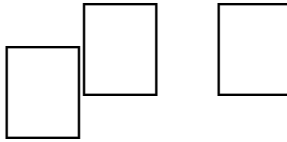


•

•

•

•



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.

The Conventions on criminal matters are widely ratified among the 89 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 60 States, or the Budapest Convention on Cybercrime, ratified by 30 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 effective. 161(;)0.444461(0)0.444461() - 1 1868(t) - 4 .05 - 4 .2735

internet companies, such as internet service providers, communications services and content (hosting platforms, to e0ec!te re4!ests *y la\$ enforcement entities in a proper, e0pedited and effecti+e manner?

)hese model information re4!est forms \$ill *e *ased on similar general principles as the ' #A model re4!est forms, partic!larly that they \$ill try to find !niform standards, facilitate operational engagement, and help a+oid incomplete or !n\$or/a*le re4!ests?

It is clear that p! *lic/pri+ate cooperation is essential \$hen it comes to the r!le of la\$ in cy*erspace, *e it in relation to terrorism, cy*ercrime or e+idence in the clo!d, and the Co!ncil of &!rope aims to ma/e life easier for *oth state instit!tions and pri+ate companies?

Aithin the frame\$or/ of the B!dapest Con+ention on Cy*ercrime \$hich has *een the leading treaty on Binternational cooperation in

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, often, multiple or shifting jurisdictions.

Traditional 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 Working Group were discussed by the Committee and by the international High Level Conference from 18 to 19 November. The results are as follows.

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

Will the Cybercrime Convention Committee hopefully decide in late 2019 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 thriving. It is able to address complex challenges, including in relation to the terrorist misuse of information technologies, while at the same time ensuring that the rule of law requirements are met.

International cooperation 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.