**IAP**

**“Introduction of Practical Guide for Requesting Electronic Evidence Across Borders from Private Communication Service Providers”**

*Monday, 16 September 2019,*

**Statement of**

**Marc Porret,**

**Legal and Criminal Justice Coordinator,**

**Counter-Terrorism Committee Executive Directorate**

***Dear Prosecutor-Generals, Attorney General, ladies and gentlemen,***

**It is an honour for me to address you all here, this afternoon.**

**I would like to begin by thanking our partners longstanding partners, the United Nations Office on Drugs and Crime and the International Association of Prosecutors.**

***Excellences, ladies and gentlemen,***

**A vital part of the international community’s counter-terrorism effort is bringing perpetrators of terrorist acts to justice and holding them accountable for their actions in accordance with the rule of law and human rights.**

**And, of course, in order to do so, prosecutors need evidence.**

**This can be either intelligence that must be transformed into evidence admissible in court, digital data, or evidence gathered on the battlefield.**

**As global connectivity has increased, terrorist groups have become more sophisticated in their use of the Internet and their use of information and communications technologies, in general.**

**And this presents law enforcement authorities with formidable challenges.**

**Member States have increasingly turned to the private sector for assistance, and we all face an ever-increasing demand for electronic evidence.**

**In the year 2017, Google received 298,235 government requests for content removal, and Facebook 42,330.**

***Excellences, ladies and gentlemen,***

**There can be no impunity for terrorist acts.**

**The Security Council has affirmed on numerous occasions that those responsible for committing, organizing, or supporting terrorist acts must be held accountable.**

**In its resolution 1373, adopted in 2001, the Council decides that Member States shall afford one another the greatest measure of assistance in connection with criminal investigations or criminal proceedings relating to the financing or support of terrorist acts, including assistance in obtaining evidence in their possession necessary for the proceedings.**

**In four recent resolutions – resolutions 2322 (2016), 2331 (2016), 2341 (2017) and 2396 (2017) – the Council calls on Member States to collect and preserve evidence to facilitate investigations and prosecutions to hold to account those responsible for terrorist attacks.**

**Resolution 2396 “*encourages* enhancing Member States’ cooperation with the private sector, in accordance with applicable law, especially with information communication technology companies, in gathering digital data and evidence in cases related to terrorism and foreign terrorist fighters”.**

**Resolution 2322 specifically notes “the significant increase in the requests for cooperation in gathering digital data and evidence from the Internet” and stresses “the importance of considering the re-evaluation of methods and best practices, as appropriate, in particular, related to investigative techniques and electronic evidence”.**

**Resolution 2322 also directs the Counter-Terrorism Committee, with the support of CTED, to work with the member entities of the Counter-Terrorism Implementation Task Force, in particular UNODC, to identify areas where it is appropriate to deliver technical assistance to Member States, upon their request, to implement the resolution.**

**This may include the training of prosecutors, judges and other relevant officials involved in international cooperation, particularly by providing analysis on capacity gaps and recommendations based on CTED’s country assessments.**

**The CTC has tasked CTED to determine whether States have effective and independent mechanisms in place to oversee the work of law enforcement agencies, with a view to ensuring professionalism and respect for human rights in their counter-terrorism work.**

**Independent and effective oversight is indispensable to ensure full respect for the right to privacy.**

**CTED is committed to the promotion of cross-border cooperation and communication to ensure the effective and speedy use of digital evidence.**

**It is also committed to the promotion of public/private partnerships.**

**The Global Internet Forum to Counter Terrorism aims to make the consumer services hosted by its member platforms hostile to terrorists and violent extremists.**

**And, in partnership with the GIFCT, the *Tech Against Terrorism* initiative has launched the Knowledge-Sharing Platform (or “KSP”) to facilitate the transfer of knowhow among established and start-up tech companies.**

**The KSP also helps prepare start-up companies to effectively respond to demands for electronic evidence.**

**Acting in accordance with Security Council resolution 2396 (2017), we shall also continue our close cooperation with UNODC and the International Association of Prosecutors, with the support of France, Germany, Japan and the United States, to help prosecutors and investigators obtain digital evidence.**

**We would welcome the engagement of more Member States in this initiative, which we consider to be a highly effective way to assist Member States to negotiate the very difficult challenges that they face in this area.**

**We are also committed to engaging with more Internet service providers.**

**More specifically, we aim to support our private-sector partners to designate 24/7 focal points to cooperate with investigators, Central Authorities and prosecutors in the preservation of evidence.**

***Prosecutor-General, attorney-generals, ladies and gentlemen,***

**We must be constantly aware that terrorists continue to adapt their tactics and strategies in exploiting ICT.**

**We believe that the launch of our “Practical Guide For Requesting Electronic Evidence Across Borders” is an important step towards further cooperation.**

**Another important challenge relates to securing evidence from conflict, post-conflict, or high-risk situations.**

**Mindful of the threat posed by terrorists, including foreign terrorist fighters and those returning or relocating particularly from conflict zones to their countries of origin or nationality, or to third countries, CTED, UNODC and the UN Global Compact CFT and Legal and Criminal Justice Working Group are developing UN guidelines to facilitate the use and the admissibility as evidence of information preserved, collected and shared by the military to prosecute terrorist offences before national courts.**

**The guidelines will be finalized shortly. They seek to strengthen the prosecution of alleged terrorists by addressing the challenges faced in exceptional situations in which criminal justice actors cannot perform their tasks.**

**They will aim to facilitate the use and the admissibility of information collected, identified, handled, preserved, and shared by the military as evidence before a national criminal court.**

**Significant information can be retrieved in conflict, post-conflict or high-risk situations.**

**Examples of such information include:**

* **Documents containing information about membership of terrorist organizations or the criminal conduct engaged in by such organizations n as a matter of policy and practice**
* **Intelligence collected by the military for operational purposes**
* **Cell ‘phones, computers, and forensic information, such as fingerprints from improvised explosive devices or weapons retrieved from the battlefield**
* **Statements of victims and witnesses.**

**Information and evidence must be gathered by the military in strict accordance with applicable domestic laws and in conformity with international humanitarian law and international human rights law.**

**However, law enforcement actors, prosecutors and judges face formidable challenges in their efforts to ensure that the information retrieved by the military – whether national, foreign or international - in these insecure situations meets the legal threshold for admissibility as evidence in criminal proceedings.**

**To be admitted as evidence, the information must meet the legal criteria set forth in IHL, IHRL, and national criminal law - including, in most domestic cases, the criterial for the proper preservation of evidence and its chain of custody.**

**Let me assure you that we at CTED will continue to play our part.**

**And I trust that we may continue to count on your support.**

***Thank you.***