Avenues for Working Group 3 to explore

The following table presents the range of possible solutions that were set out by participants both at the first Working Group 3 meeting and at the second HLG Plenary which can be developed upon in the second WG3 meeting according to three main solution areas:

Problem breakdown	Avenues to explore

Lawful interception **of electronic data**
 	
[This discussion item does not cover end-to-end **encryption of content data**, which brings challenges of a different nature, thus is addressed separately]
	• Exploring the conditions for real time lawful access for Internet service providers:
	  ○ Clarify the legal situation in light of the EECC
	  ○ Clarify the interplay with data protection rules (GDPR), ePrivacy, the e-evidence package as well as international conventions.
	  ○ Assess the interplay with national laws on LI,
	  ○ Agree on common requirements for real time interception.
	  ○ Explore conditions that protect fundamental rights and addresses conflicts between national laws including reflections on:
	  ▪ Overall organisation e.g. "to which extent is the e-evidence model applicable?"
	  ▪ Type of interception (e.g. only targeted, categories of crime, duration, categories of data, etc...)
	  ▪ Dealing with geolocation of targets,
	  ▪ Dealing with the possible encryption of meta data,
	  ▪ Judicial authorisation and review,
	  ▪ Notice to targets,
	  ▪ Transparency reports
	  ▪ Etc...
	
	• Explore avenues to mitigate technical and legal challenges of real time interception measures implemented through MLAT or EIO expressed by MS (i.e. lack of relevant technical infrastructure to transfer real time interception).

Targeted lawful remote access to devices	• (Legal) Explore conditions for legal certainty when using special techniques to access data on devices remotely,
	  ○ Based on lessons learnt from Encrochat & Sky ECC,
	  ○ Factoring in the debate on Pegasus like approaches and the debate on vulnerability management
	• (Technical) Explore conditions for an EU industrial approach to lawful remote access.

Specific challenges posed by **encryption**.	• Explore solutions for traditional telecommunication providers in cases like:
	  ○ RCS (Rich Communication Services) that is becoming the norm to exchange SMS in an end-to-end encrypted manner,
	  ○ 5G communications for inbound roamers (when the targets are using SIM cards issued by foreign operators and applying encryption),
	• Explore solutions for non-traditional telecommunication providers notably when implementing end-to-end encryption or implementing privacy preserving architecture which prevents the identification of Internet users.