Annex A (Glossary)

- **Cybercrime:** an umbrella term used to describe two distinct, but closely related criminal activities: cyber-dependent and cyber-enabled crimes. Cyber-dependent crimes are offences that can only be committed by using a computer, computer networks, or other forms of ICT e.g. malicious software, hacking. Cyber-enabled crimes are traditional crimes that are increased in their scale or reach by the use of computers, computer networks or other ICT e.g. fraud, theft.
- **Cyber resilience:** being able to prepare for, adapt to, withstand and rapidly recover and learn from disruptions from cyber criminality/attacks. To do this, people need to develop the skills, knowledge and understanding of the risk, in whatever setting they find themselves in, and then take the necessary steps to prepare for and respond to such events.
- **Cyber security:** the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets
- **Cyberspace**: Cyberspace is the complex environment that results from the interaction of people, software and services on the Internet by means of the technology devices and networks connected to it, which does not exist in any physical form.
- **Hacking**: breaking into computer systems