Glossary

Cybercrime: can include acts against the confidentiality, integrity and availability of computer data or systems. It can also encompass computer-related acts that result in personal or financial gain or harm, such as identity theft. Generally, cybercrime is categorised as cyber-dependent crime (a cybercrime that would not be possible without the Internet and digital technologies) and cyber-enabled crime (a cybercrime facilitated by the Internet and digital technologies).

Darknet: part of the Internet that is purposefully not open to public view. Websites use anonymity tools like TOR to encrypt their traffic and hide their IP addresses. The high level of anonymity enables criminals to act without being easily detected. As a result, websites host and offer illegal activities, goods and services.

Deep Web: part of the Internet that is not discoverable by search engines and is not easily accessible by or available to the public. It includes password-protected information, from social networks to email servers.

Organized criminal group: The Convention against Transnational Organized Crime defines an organized criminal group using the following criteria:

- A structured group of three or more persons
- A group that exists for a period of time
- A group that acts in concert with the aim of committing at least one serious crime
- A group that acts to obtain, directly or indirectly, financial or other material benefit

Participation in an organized criminal group: The Convention against Transnational Organized Crime defines participation in an organized criminal group in two ways: conspiracy and criminal association. These offences create criminal liability for persons who intentionally participate in or contribute to the criminal activities of organized criminal groups.