(B) General Questions
(1) No such common definitions exist.
(2) Within the police organisation there are special units for ICT-intelligence, i.a. a unit for collecting information on the Internet. As to the technical development, most public agencies have their ICT-units.
(3) Apart from technical maintenance and development, no such services exist.

(C) Information and Intelligence: building information positions1 for law enforcement
(1) Building information positions is performed mainly by the Police by collecting information on the Internet and other open sources.
(2) All open (public or private) databases are available to the police and other law enforcement agencies.
(3) Both techniques are possible and are used. They can be used to create profiles and risk groups. Not known whether special tools have been developed.
(4) No.
(5) Providers of communication nets are obliged to store data during six months.
(6) No (apart from 5 above)
(7) Police and prosecutors are under the general control of the Swedish Data Inspection Board (focuses on protection of the integrity of individuals). The Commission on security and Integrity protection controls how the Police use wiretapping and other forms of secret supervision as well as their processing of personal data.

(D) ICT in the criminal investigation
(1) Swedish law enforcement agencies can carry out interception in real time of both e-traffic data and content data.
(2) Swedish law enforcement agencies can only have access to information systems for e-traffic data and content data through the use of search and seizure. According to Swedish law search and seizure cannot be used to get information from a service provider. To get information from a service provider (apart from subscriber information) secret tele-surveillance or interception has to be ordered.
(3) Under Swedish law service providers can be obliged to share data with law enforcement agencies, through the use of secret tele-surveillance or interception. When it comes to subscriber information, however, a service provider can be ordered to hand out such information. The breach of the duty to cooperate can result in an order to take corrective actions at the risk of liquidated damages and can, ultimately, have the effect that the service provider no longer is permitted to carry on his business.
(4) Swedish law enforcement agencies may apply video surveillance. They can not oblige natural nor legal persons to cooperate.
(5) Swedish law enforcement agencies may apply audio-visual recording of interrogations but must not.

(E) ICT and evidence
(1) There are no Swedish rules on evidence that are specific for ICT-related information.
(2) There are not any Swedish rules on integrity and security of ICT-related evidence.
(3) There are not any Swedish rules on admissibility of evidence that are specific for ICT-related information. Generally, there are no rules on admissibility of evidence in Swedish law. In Swedish law there is a principle of free evaluation of evidence.
(4) There are not any specific Swedish rules on discovery and disclosure for ICT-related evidence.
(5) There are not any special Swedish rules for evaluating ICT-related evidence.

(F) ICT in the trial stage
(1) There are no specific Swedish rules on how ICT related evidence can or must be introduced in the trial.

* Important notice: this text is the last original version of the national report sent by the author. The Review has not assured any editorial revision of it.
(2) Distant interrogations can be applied at a Swedish trial, and it is quite common that this kind of technique is applied.
(3) Digital and virtual techniques can be used for the reconstruction of events at a Swedish trial.
(4) Audio-visual techniques can be used to present evidence at trial in Sweden.
(5) The last years there has been an on-going project to replace criminal “paper” case files by “electronic ones” in Sweden. Hence, there are major developments towards digitalising of the trial proceedings in Sweden.