11/ Phone Tracking and Surveillance

Things to consider

Mobile phones are invaluable resources for work and can also be of great use for security: in an emergency situation, they are the first tools that many will reach for. However, they do have vulnerabilities.

- A mobile phone is like a tracking device: its **location is constantly communicated** to the company that runs the network. Even this basic location data has been used by authorities to identify and harass participants in protests as well as for general surveillance.
- 'Normal' phone calls through the mobile phone network, as well as SMS messages, are transferred across the network without much encryption. This means that they can be recorded, listened to, stored, and read easily by those who control the network. Third parties can also use tools such as **IMSI catchers** to 'listen in' on the phone calls and SMS messages passing through.
- Smartphones have hardware features that can facilitate surveillance such as GPS and batteries that cannot be removed. Smartphones are often the subjects of **targeted malware** attacks, which can essentially make them remotely controlled.
- Some apps such as voice-activated personal assistants may expose users' private lives to the opportunistic **surveillance of the large tech companies** which run them, and whomever they are legally obliged to share their collected information with.

Protection tactics

- **Avoid normal calls and SMS**: only use them to exchange sensitive information in exceptional circumstances, such as in emergencies.
- Use a **Faraday bag** to block your device from the mobile network and obscure your location (at least via the mobile network) and block radio signals. Keep in mind that a Faraday bag does not prevent the microphone from functioning and recording, and that Bluetooth and Wi-Fi should be switched off manually.
- Check whether HRDs are comfortable keeping their mobile phones with them before meeting with them and **leave devices in a different space** out of earshot of your conversation.
- Install and use a **Virtual Private Network (VPN)** on your phone.
- Exercise extreme **caution with any links or files** that are shared with you via SMS or messaging services, and do not open them unless you were **explicitly** expecting them.
- **Switch off all apps** that might be abused for recording conversations, such as Skype. **Remove** apps that you do not actively use from your phone.