5/ Secure Calls, Chat, and Email

Things to consider

- When communicating with someone via an online platform, both the **content** of the communication (the messages) and the **meta-data** (information about the devices, the app, and the communication) travel through a number of different points, often all over the globe.

- This includes routers, the infrastructure controlled or rented by Internet Service Providers (ISPs), national gateways often controlled by the State, Internet Exchange Points, etc.

- When data is sent **unencrypted** across these channels, it can be read by people with access to any of these many points.

- Many email providers and messaging apps encrypt content now using a protocol known as Secure Socket Layer (**SSL**). This can be seen as **"https"**, such as when browsing websites. This provides some protection, but can not be trusted on its own for secure communications.
  - ○ SSL encryption does not protect data from being read by the owner of the website or app, such as many free email providers, and social networks. They can access content and data either for their own interests, or when requested by authorities.
  - ○ SSL is a common target for those trying to **eavesdrop** on communications or access other sensitive data.

Protection tactics

- Always discuss the potential risks posed by communication between embassy staff and HRDs at the start of any cooperation. Decide about apps and channels to use based on this assessment.

- Sensitive communications require services, tools, or applications with **end-to-end encryption**, that ensure only the sender and recipient(s) of an email, message, or call are able to decrypt it. Some messaging, call, and video services provide this by default. However, in some contexts they are illegal or attract further attention.

- Look for apps that implement "**Perfect Forward Secrecy**" and 'disappearing' or 'self-destructing' messages. Perfect Forward Secrecy is a security feature which ensures that intruders can only decrypt one message at a time. **Self-destructing messages** 'disappear' after a certain amount of time, or can be deleted by users from their own and their interlocutors' devices. However, it is not clear to what extent these messages can be recovered.

- Some HRDs use **PGP** encryption on their emails. If this is not possible, move all sensitive discussions to an encrypted messaging application. Email attachments can be encrypted and the password should be shared over a secure third channel.