4/ Connecting to the Internet Securely

Things to consider

In certain areas and contexts, the very act of connecting to the internet – as an embassy staff member working on human rights, or as a human rights defender – can be a threat to your information security:

- Network administrators, opportunistic criminals, Internet Service Providers (ISPs) and even State agencies may be **monitoring** internet users, and looking for vulnerabilities to exploit.
- Wi-Fi networks in **public places or hotels** can be closely monitored by the network administrators, as well as by the parties mentioned above.
- On public Wi-Fi, **unencrypted content** sent over the internet, such as the content of webpages that do not have an SSL (or "https") connection, as well as metadata (such as visited websites) is vulnerable to being accessed in these cases.
- Wi-Fi networks might also be used to install **malicious software** on devices. Examples are known of journalists, NGOs, or political opposition being targeted in this manner.
- At workplaces or at home, routers used to connect to the internet may have insecure **firmware**, allowing for access by adversaries. They can enable routers to store data about your internet use or facilitate its handover to third parties.

Protection tactics

- Install and use a **Virtual Private Network** (VPN) on your mobile devices and computers to hide the relationship between your device and your online activities. Some VPNs have been made with HRDs in mind and can be recommended to them in these cases.
- Connect to your mobile network by creating a **hotspot or tethering** from your phone, and avoid connecting to the provided network when in public places where you suspect there might be a likelihood of network monitoring by authorities or even a risk of malware infection.
- Consider using **Tor Browser**, also available as an app, which routes your data through a combination of at least three nodes in the Tor Network, facilitating access to blocked content and anonymity on the internet. Be aware that using Tor might trigger attention from authorities in some contexts.