10/ Targeted Malware and Other Attacks

Things to consider

- **Malicious software**, or 'malware', is any software that can cause damage to your digitally stored data, or give third parties access to it.
- HRDs, politicians, journalists, and the diplomatic community must be aware of the threat of malicious software designed specifically for espionage on them.
- This **targeted malware** typically allows **remote control access** to all files on the device, as well as the ability to record all keyboard uses or switch on the camera and microphone, without alerting the user to what is happening.
- This kind of infection with malware happens in several ways, including **links or attachments** sent via messaging services or email which download the software to their devices once clicked or opened. **Wi-Fi access points** and business centres in hotels frequented by 'targets' are sometimes used to infect them with malware.
- Another targeted attack commonly used against civil society is known as '**phishing**'. Phishing means using cleverly designed emails or false websites to trick users into clicking on a particular link, downloading a programme, or giving their login or other details to an attacker.

Protection tactics

- Installing an **anti-malware** programme on all devices is a vital basic practice. Remember to keep software updated.
- Use **link expanders** to see the real addresses of suspicious, shortened URLs.
- Make **regular backups**, ideally daily, or at least weekly. This greatly reduces the impact of data loss, which can also be caused by malware, or ransomware. Make sure that any encrypted data is also backed up in encrypted form.
- Use communication applications which allow for **verification** of device **'fingerprints'** – and verify the 'fingerprints' of your contacts' devices.
- Do not connect to **public Wi-Fi** offered in hotels, conference venues, or other places frequented by civil society, journalists, dissidents, or opposition politicians.
- When you are subjected to a targeted malware attack or suspect you have been, contact your local IT support as soon as possible and raise the issue as appropriate within the office.