Operational Security

* The internet
* Threats posed
* Devices
* Data
* Communication
* Resources

## Attack Surface

* Data location
* Moving data
* Protection at each location (backups etc.)
* Jurisdiction

Peer to peer – each node on the internet becomes it’s own ‘server’ and can talk to other nodes.

Storing data in different countries have different legal jurisdiction.

## Encryption

* Cryptography
* Transport Encryption
* End to end encryption

## Authentication

* Out of band – second factor authentication
* Web of trust – multiple people can authenticate each other
* 2 Factor

## Anonymity

* Hide in the crows
* Meta-data
* Operational Security – you can be identified by your behaviour

## Content / Meta-data

## Proprietary (Code is not released) / Open Source / Free Software (Licensed)

## Threats / Malware

* Platform (Vulnerability / Supplier)
* Arms Race (Virus protection getting info of new viruses)
* Stuxnet

## Interception

* Blanket
* Jurisdiction
* Five-eyes
* Meta-data - even encrypted data can show meta-data

## Hacking

* Intelligence Service
* Crime
* Anonymous – info release

## Theft

* Remote encryption/blackmail
* Off-line
* Miranda – (Seizure)
* DPR

## Hardware

* Hardware - Hardware can already have
* Source (distributor)

## OS

* Closed/Open/free
* Disk encryption
* Package authentication
* Licence agreement
* Linux tails – privacy and anonymity

## Software

* Source
* License Agreement – closed – open source – free
* Authentication
* Reputation

## Password Security

* Non-Obvious, length, complexity, non-personal
* Do not reuse
* Periodic Reset

## Backup

* Regular
* Encrypted
* Location

## Instant Messaging

* Protocol
* End-to-end encryption
* Authentication – public private key
* Platform
* Applications: Signal & Conversations(OTR)
* Email – Transport Encryption TLS – GPG

## Browsing

* Browser plugin – do not track, script blocking
* SSL
* Tor – bounces data around the ‘cloud’
* Some don’t allow exit nodes etc.