Michael Anders

Surveillance and the Art of Digital Camouflage

**57 exercises
to escape the dragnet
of surveillance.**

- Only a simple Windows or Linux computer required.

- Predicted working time for all exercises.

- Clear division into four skill levels.

- Enables to make good own decisions.

- Exercises get more challenging with increasing reader progress.

Use TOR in rendezvous mode:
The communication does not require any resources outside the TOR anonymization network. Sender and recipient connect directly via TOR.
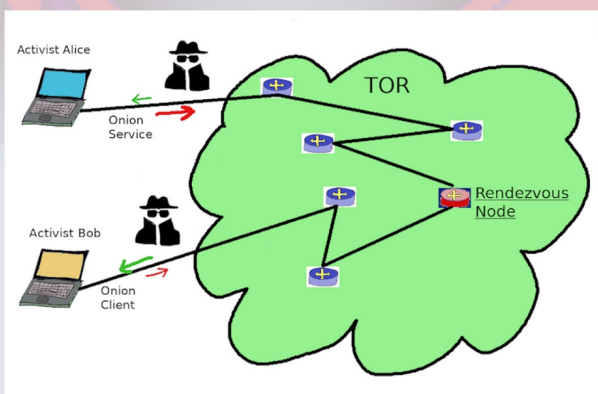
Not least since the disclosures of Edward Snowden, we are aware of the ubiquitous collection of our data for commercial and political purposes. However, we are not helplessly at the mercy of the eavesdroppers collecting and aggregating our data against our will.

This book shows how we can protect our sensitive communication even against seemingly overpowering opponents.

In western democracies, the protection of private communication can be a means of preventing further slippage into the surveillance state.

In a threatened or already damaged democracy, the protection of computer-based communication can even be a means of self-protection for critical organizations and dissidents. Lawyers and journalists with powerful, even nation-state adversaries should be able to master such secure communication for the protection of clients and sources.

In this book, we reach the peak of protection in Internet communication. The powerful surveillant cannot uncover who the sender of an intercepted message is or who the intended recipient is. Furthermore, the surveillant cannot gain any information about the type of encryption applied to the intercepted message or whether it is an encrypted message at all. It looks like pure digital noise to the surveillant. All it can find out is that someone may be communicating with someone else via its network infrastructure.