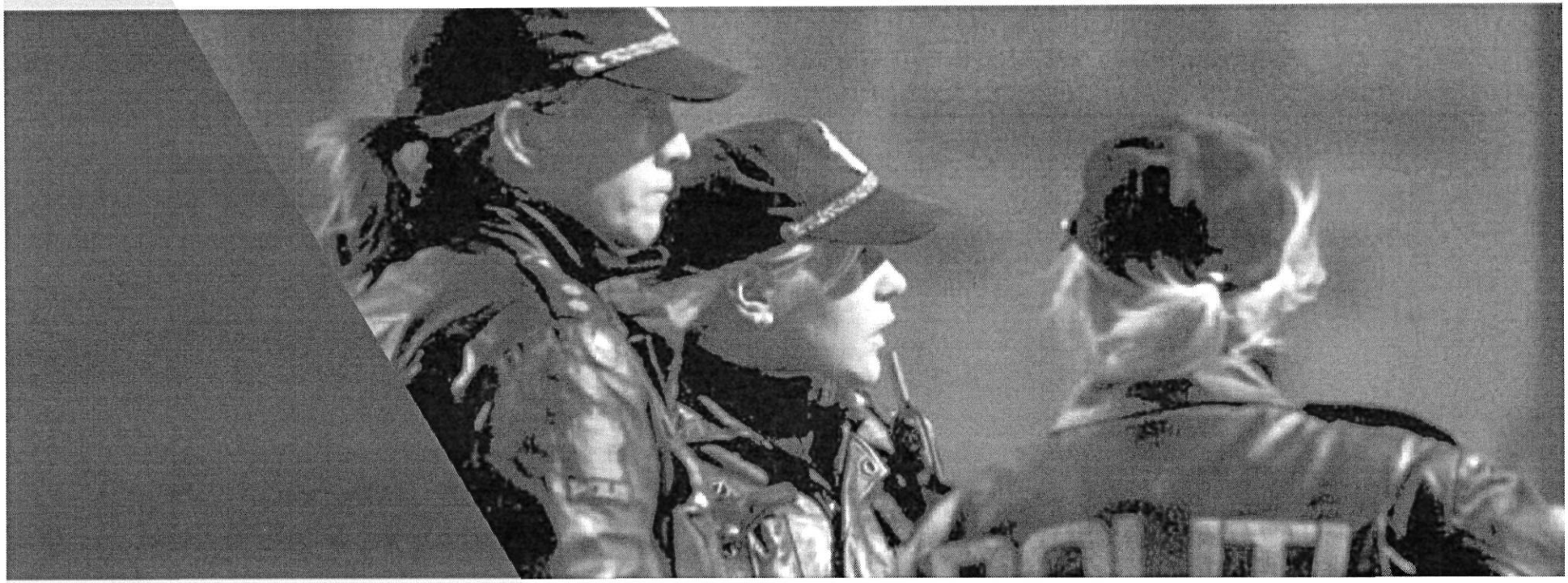
POLITIHØGSKOLEN



Police practices on the TOR-network: Some legal questions to be addressed

Introduction

1 The main focus in this presentation
2 The legal framework
3 The use of hacking tools by law enforcements

Dan Alfin, special agent, FBI Violent Crimes Against Children Section:

"It's the same with any criminal violation: As they get smarter, we adapt, we find them. It's a cat-and-mouse game, except it's not a game. Kids are being abused, and it's our job to stop that."

- **Is using TOR legal?**

- **Is using TOR for the good?**

  It protects the principles of human rights. ECHR Art 10. *Freedom of expression* and art 8. *Right to respect for private and family life*

  The TOR protect users from two types of surveillance. First it protect users by traffic analyses, and second it prevents governments from using the metadata (information about a communication).

  It protect the freedom of speech for civil liberties advocates, journalists, whistleblowers among others.

The legal framework

- **The legal framework;**

  1 **Convention on Cybercrime**

  2 **European Convention on Human Rights (ECHR)**

  3 **EU law**

  3 **National substantive and procedural laws**

Convention of Cybercrime

Is the main legal instrument of the internasjonal legal framework of cybercrime. It has a wide range of substantive, procedural, and mutual-assistance provisions.

Restriction pursues legitimate aims: Prevention of crime, protection of national security/public safety and protection of economic well-being of the country.

Restriction must be precribed by law.

European Convention on Human Rights (ECHR)

Law concerns when policing on TOR

- The police are TOR-users as undercover agents.
- In any case, the police have to respect the national procedural laws for provocation and infiltration.
- The use of TOR network by criminals to anonymize communication makes it impossible for law enforcements to find the criminal subjects just using ordinary investigative methods.
- The most common way for the police to investigate crime on TOR is to join the TOR network and look for faults.
    - Bitcoin
    - Marketing
    - Communications

Surveillance methods in Norway

-Communication monitoring (including traffic data, IMSI catcher, hidden sms)

-Data security

-Audio surveillance

-Data reading (governmental hacking)

-Camera surveillance in public and private locations

-Release orders, search warrants and seizures without notification.

Law enforcement hacking at TOR

***The Criminal Procedure Act,* Act of 22 May 1981 no. 25:**

§ 216 o. ***The court may make an order permitting the police to carry out computer search when any person is with just cause suspected of an act or attempt at an act.***

The Criminal Procedure Act § 216 o and § 216 p

What is a computersystem;

-Objects consisting of hardware and software

-User accounts for network-based communications and storage services

- Requires identification of the datasystem

- Requires a link to the suspect

What is computer search according to the norwegian law;

"Communication, electronically stored data, and other information about the computer system or user account".

In what way;

"using technical facilities, computer programs or otherwise.

"can be installed in the computer system and in other hardware that can be connected to the computer system".

"may break or bypass protection in the computer system".

Legal aspects of jurisdiction

- **Are there international difficulties with the use of governmental hacking-methods to investigate internet users who have used anonymizing software to twart law enforcement investigations?**
- **Does governmental hacking-methods violates international laws?**
- **To what extent should national police be able to use information obtained by methods that are not allowed in their own country?**


POLITIHØGSKOLEN