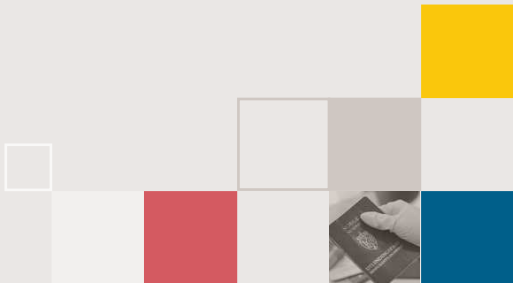
POLITIET

NCIS
National Criminal Investigation Service

Regional Workshop on Cybercrime: The experience of Norway in investigating cybercrime and implementing the Council of Europe Convention on Cybercrime

Eirik Trønnes Hansen
police prosector

"The national competence center in the fight against crime"

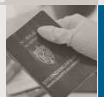


POLITIET

NCIS
National Criminal Investigation Service

Cybercrime vs electronic evidence in other cases: The experience of Norway

- Electronic evidence such as internet records may be used as evidence in any criminal case, not just cybercrime.
- Mobile phone records are used as evidence significantly more often than internet records.
- The majority of cases where digital data forensics are used as evicence, are not cybercrime cases.
- Cybercrime cases are usually based on internet records, digital forensics (analysis of the computer used by the suspects) and statements from the complainant.

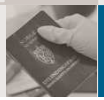


POLITIET

NCIS
National Criminal Investigation Service

Cybercrime: some cases handled by NCIS Norway

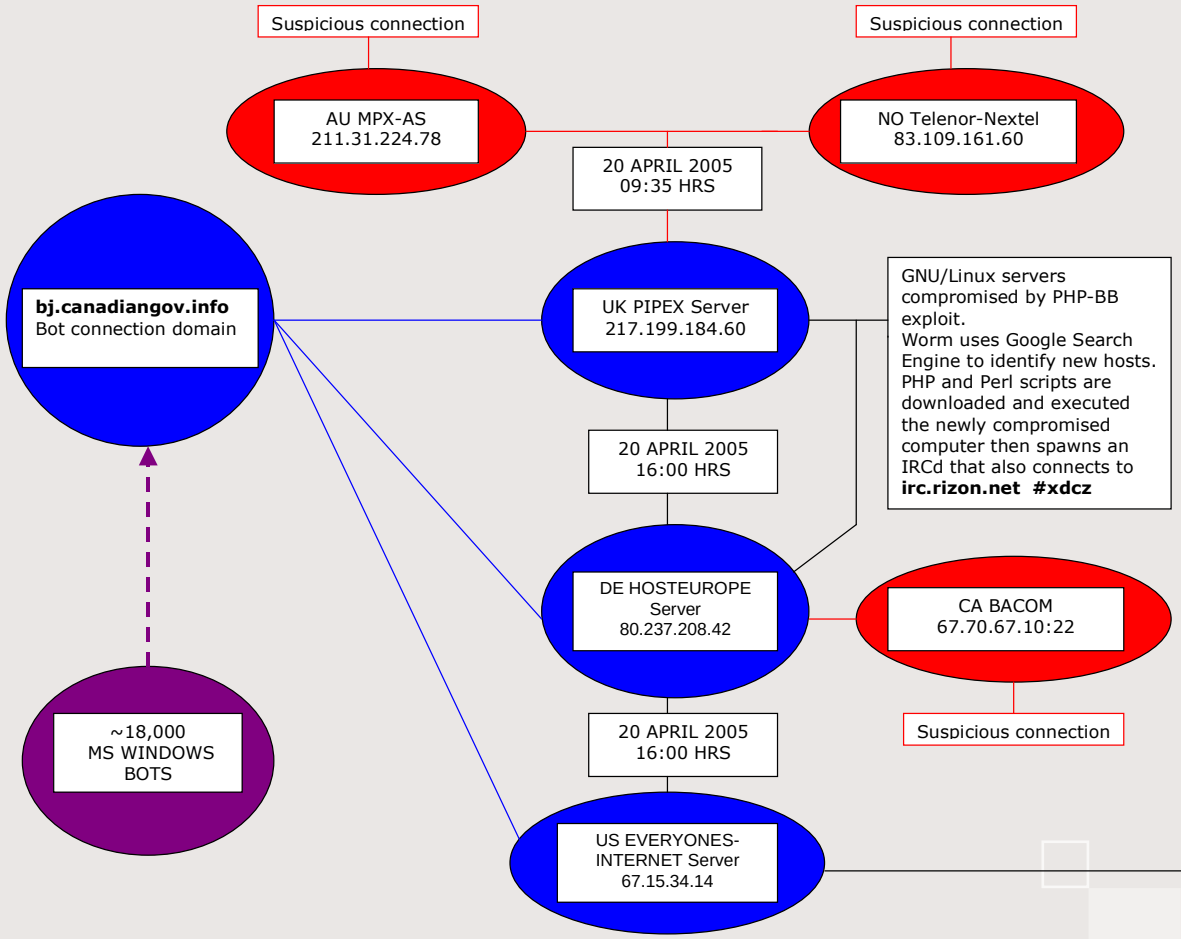
- ”Hacking”: Computer break-in, DDoS, botnets etc
- Internet banking fraud
- Phishing
- Intellectual property crimes
- Threats and harassment via the internet (Example: treats of school shootings posted at Facebook or YouTube)
- Child abuse images



POLITIET

NCIS
National Criminal Investigation Service

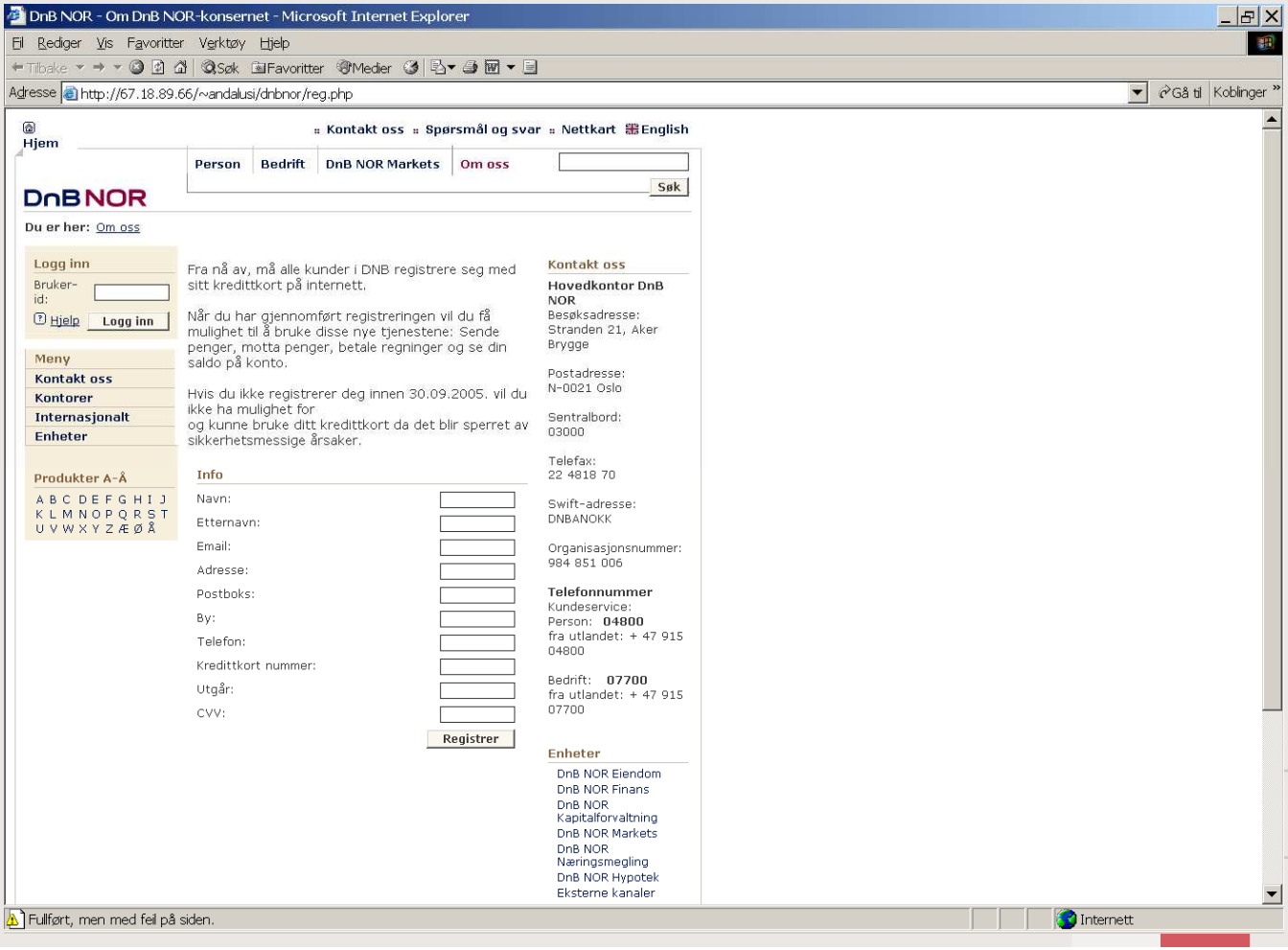
Botnet: case example



POLITIET

NCIS
National Criminal Investigation Service

Phishing: case example



POLITIET

NCIS
National Criminal Investigation Service

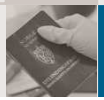
Case example: internet banking fraud

POLITIET

NCIS
National Criminal Investigation Service

Case example: internet banking fraud

- An ongoing international problem.
- 2006-2008: at least 100 Norwegian internet bank customers had their computers infected by malware (password stealing trojans), that made it possible for third parties to illegally access their internet bank accounts and transfer money to other accounts.
- The money were transferred to other Norwegian bank accounts. These accounts were owned by people who had previously agreed to help others in money transactions (”money mules”). The ”mules” were rectruited via internet ads (”make money at home”). From their accounts, the money were transferred out of Norway via Western Union.
- Several ”money mules” have been convicted for money laundering, but the prime suspects are outside Norway, and are still at large.

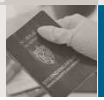


POLITIET

NCIS
National Criminal Investigation Service

Case example: internet banking fraud

- During the Norwegian investigation (2006-2008), NCIS Norway cooperated with 20 countries, in part via Europol.
  - The FBI helped secure data from several websites, that had been used for spreading malware. The files were analysed by NCIS Norway. The FBI also helped secure contents from a website used to recruit ”money mules”.
  - Daily/weekly contact with UK police
- 5 NCIS detectives on the case (tactical and technical)
- Analysis of more than 30 computers.
- Cooperation with external parties like Microsoft, virus detection providers, Certs, financial sectors.

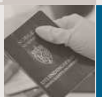


POLITIET

NCIS
National Criminal Investigation Service

Case example: ”Operation Enea”

- In May 2004, NCIS Norway cooperated with police in Denmark and several other countries in an large scale investiagion regarding child abuse images.
- 850.000 identified child abuse images at the file sharing network Kazaa were monitored for three days. These images were connected to 14.500 IP adresses world wide.
- In Norway, this investiation led to 253 criminal cases with 149 convictions. 49 cases were eventually closed.
- 43 cases opened in Denmark
- Cooperation with police via Interpol in several other countries.

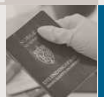


POLITIET

NCIS
National Criminal Investigation Service

Case example: ”Operation Enea”

- Cooperation with police in several other countries. The cooperation was largely limited to transfering cases from Norway to other countries.
- 43 cases opened in Denmark
- One Enea case was tranfered to the Australian Federal Police. Through this investigation, it was discovered that the suspect was sexually abusing three young children in his family.
- One Enea case was transfered to the police in Texas, USA, who discovered that the suspect had been abusing children. The suspect was sentenced to 15 years prison for that offence.

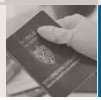


POLITIET

NCIS
National Criminal Investigation Service

- *Gentlemen, greetings from Texas! Hope you are doing well. I wanted to update you on one of my Op Enea cases.*

  My Enea target, --- (enea ID 116602), is currently pending indictment. The computer forensic report is almost complete and shows that --- had about 5,000 images of child porn on his computer, including images of bondage, rape, and infants. After the forensic report is finished, I will be contacting the prosecutor about indicting --- on the federal charges. You will be interested to know that during a polygraph exam on this case, --- confessed to child molestation. The victim was identified and located, and --- was arrested on charges of Aggravated Sexual Assault of a Child. --- was sentenced to 15 years prison on June 20, 2005 for that offense. After we indict --- on the federal child pornography case, he will be transferred to federal custody to await sentencing/trial. Good job catching this guy! He was living in a trailer park adjacent to a city park, where children play every day. He was also on probation for state charges of Possession of Child Pornography



POLITIET

NCIS
National Criminal Investigation Service

Operation Enea: final analysis

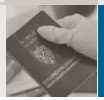
- The police investiation was internet related (IP tracking etc), based on digital forensics (analysing the computers used by the suspect) and based on other, traditional police methods.
- NCIS Norway had a good cooperation with police and prosecutors in other countries.
- The individual cases in Norway were transfered to the local police and local prosecutors because of the large number of cases.
- What could have been done differently?
- Would this project have been possible in Norway today?
  One problem: IP logs are now deleted by the ISPs in Norway after 0 to 21 days. No current obligation to store traffic data.

POLITIET

NCIS
National Criminal Investigation Service

Main Tasks for NCIS Norway

- Investigate and prosecute serious and organised crime, including computer-/internet-related crime
- Co-ordinate, gather and disseminate criminal intelligence as the national criminal intelligence center
- Develop new methods and transfer competence to the police districts
- NCIS is integrated organisation with police officers, prosecutors and technical experts

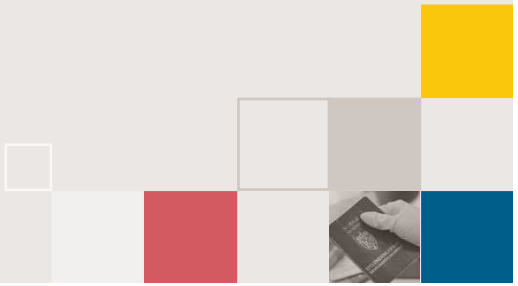


POLITIET

NCIS
National Criminal Investigation Service

International Police Co-operation

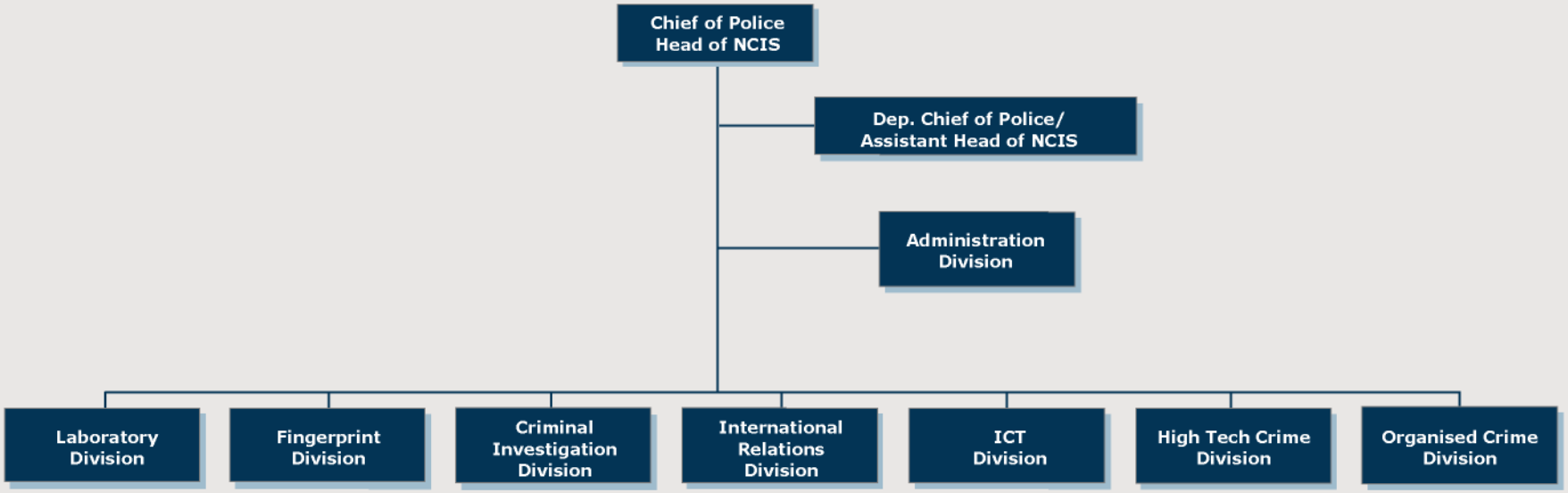
- NCIS Norway is the contact point for national and international exchange of information
- 24-hour Desk
- Interpol Oslo
- Europol
- SIRENE/Schengen
- G8 contact point



POLITIET

NCIS
National Criminal Investigation Service

Structure of NCIS Norway



POLITIET

NCIS
National Criminal Investigation Service

Royal Ministry of Justice and the Police

National Police Directorate

Police Security Service

National Criminal Investigation Service (NCIS)

National Police Computing and Material Service

National Mobile Police

National Police University College

National Police Immigration Unit

Commissioner to the Russian Border

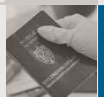
Police Districts 27

Rural police districts

Local police stations

National Authority for Investigation and Prosecution of Economic and Environmental Crime (Økokrim)

- Approx. 11,500 employees in the service (all categories)

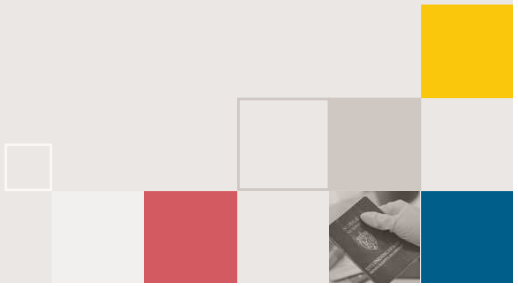


POLITIET

NCIS
National Criminal Investigation Service

Norway and the Convention on Cybercrime

- The convention was signed by Norway 23.11.2001, ratified 30.06.2006 and went into force 1.10.2006.
- In 2005, Norwegian legislation were amended to harmonise the local legislation with the convention.
- Example: article 16, expedited disclosure of stored computer data and the new article 215a in the Criminal Procedure Act



POLITIET

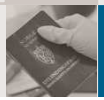
NCIS
National Criminal Investigation Service

Internet records: preservation of accounts

The Criminal Procedure Act, section 215a:
The prosecution authority may as part of an investigation make an order concerning the securing of electronically stored data deemed to be significant as evidence.

An order concerning the securing of data in a communication that is in the possession of a provider of access to an electronic communication network or electronic communication service may only be made if the conditions in the first paragraph are fulfilled and there is reason to believe that a criminal act has been committed.

The person who is entitled to dispose of the data covered by a security order shall be informed of the order.



POLITIET

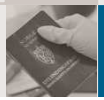
NCIS
National Criminal Investigation Service

Internet records: standards of proof for subscriber information

- The Electronic Communications Act, section 2-9:

Providers and installers have a duty to maintain secrecy on the content of electronic communications and others' use of electronic communications, including information on technical systems and methods. (…)

The duty of confidentiality does not prevent information being given to the prosecuting authority of the police on contract-based telephone numbers or other subscription information, as well as electronic communications addresses. The same applies in giving evidence in court. Nor does the duty of confidentiality prevent information as mentioned in the first paragraph being given to another authority pursuant to the law.



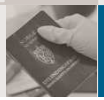
POLITIET

NCIS
National Criminal Investigation Service

Internet records: standards of proof for subscriber information

A request from the prosecuting authority or the police for information as described in the third paragraph shall be complied with unless special circumstances make this inadvisable.

Regulations relating to Electronic Communications section 6-2:
Phone service providers must register the name, address etc of their individual customers.



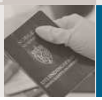
POLITIET

NCIS
National Criminal Investigation Service

Internet records: standards of proof for content

- The Criminal Procedure Act, section 203:
Objects that are deemed to be significant as evidence may be seized until a legally enforcable judgement is passed.

This includes data such as content data.



POLITIET

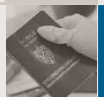
NCIS
National Criminal Investigation Service

Internet records: preservation of accounts

A suspect shall be informed as soon as the data has been secured and he has been given the status of a suspect. Otherwise information shall be given as soon as the data has been secured.

The security order shall apply for a specific period that must not be longer than necessary and not exceed 90 days at a time. If a security order is made at the request of a foreign State, it shall apply for at least 60 days. Section 197, third paragraph, 208, first and third paragraphs, and 216 i shall apply correspondingly

The person who is subject to the order shall on application surrender the traffic data necessary for tracing where the data covered by the security order came from and where they may possibly be sent.

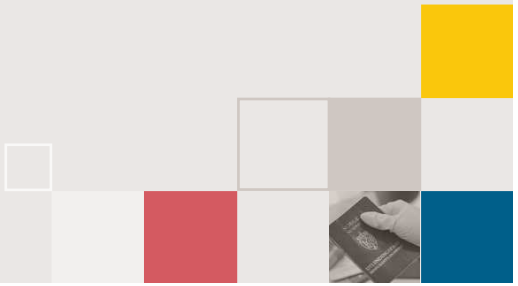


POLITIET

NCIS
National Criminal Investigation Service

Internet records: preservation of accounts

- Section 215a is in accordance with the Cyber Crime Convention, Article 16
- NCIS is the contact point for international requests regarding preservation of accounts and other data.
- Court order is not necessary.

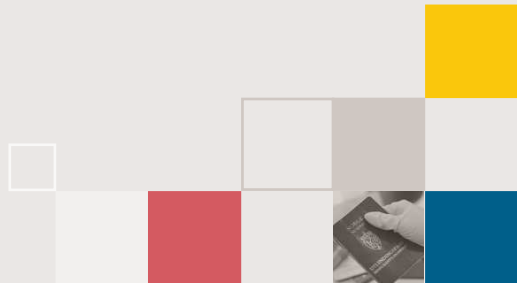


POLITIET

NCIS
National Criminal Investigation Service

Internet records: 24/7 hotline

- NCIS, High Tech Crime Division, is the G8 contact point
- 24-hour Desk



POLITIET

NCIS
National Criminal Investigation Service

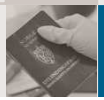
Internet records: standards of proof for content

- Section 210:

A court may order the possessor to surrender objects that are deemed to be significant as evidence if he is bound to testify in the case.

If delay entails a risk that the investigation will be impaired, an order from the prosecution authority may take the place of a court order. The decision of the prosecuting authority shall be submitted to the court for approval as soon as possible.

Section 210a: The court may order deferred information to the suspect



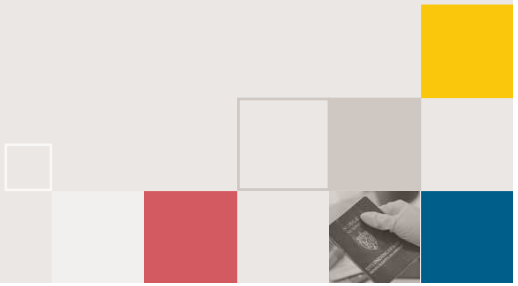
POLITIET

NCIS
National Criminal Investigation Service

Internet records: standards of proof for content

- Section 210b: Future traffic data

- Section 210c: The court may order deferred information to the suspect



POLITIET

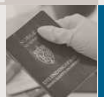
NCIS
National Criminal Investigation Service

Internet records: standards of proof for content

- Section 211:

Any letter, telegram or other communication that is in the possession of a postal agency or a provider to an electronic communication network or electronic communication service may be seized pursuant to court order if such communication may prusuant to the provisions of sections 203 and 204 be seized from the recepient and suspicion is directed to an act punishable pursuant to statute by imprisonment for a term exceeding six months.

If delay entails any risk, the prosecuting authority may order the controller of any post or telegraph office to withhold such items until the court has made its decision but not for more than one week.



POLITIET

NCIS
National Criminal Investigation Service

eirik.tronnes.hansen@politiet.no

"The national competence center in the fight against crime."