POLITIET
KRIPOS

NCIS Norway
National Criminal Investigation Service

International cooperation

Eirik Trønnes Hansen
prosecutor, NCIS Norway

GLACY conference, Dakar
24.-27. March 2014

Agenda

- Introduction
- Norway and the Budapest convention
- NCIS Norway organization and functions
- Norwegian legislation
- Three case examples
- Experiences with the 24/7 network and expedited preservation
- Conclusion

Norway and The Budapest Convention

- 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
- Norway takes an active part in the work connected to the Convention, and we hope that the Convention can be extended to more parties.
- NCIS Norway is the national 24/7 contact point.

NCIS Norway organization and functions

Core functions for NCIS Norway

- The Norwegian contact point for Interpol, Europol, SIRENE (Schengen information system) and the 24/7 network (The Budapest Convention art. 35)

- Forensic services, including digital forensics and analysis

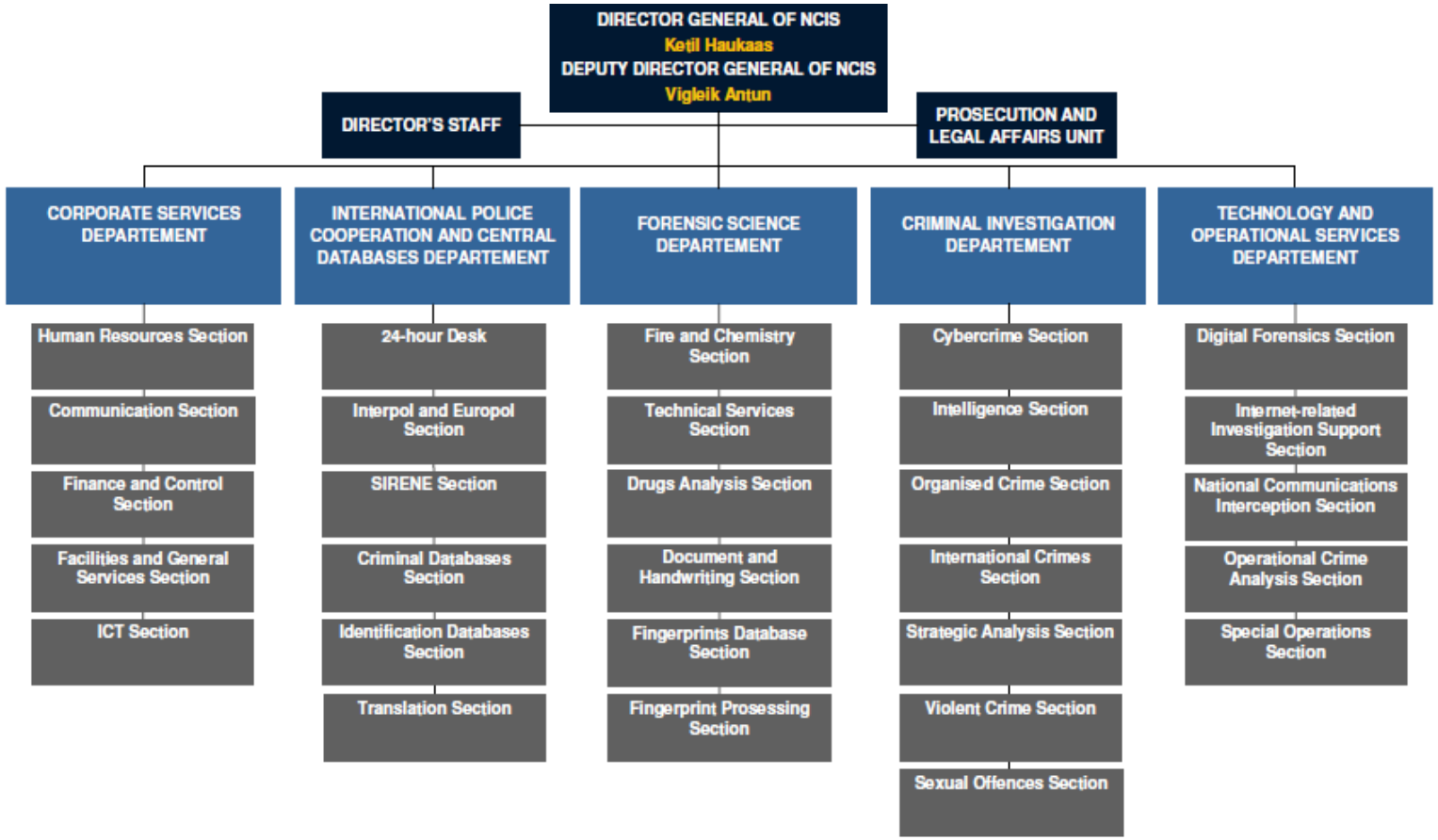
- Develop and maintain several central police databases

- **Investigating and prosecuting**
  - organised and other serious crimes
  - crimes against humanity and war crimes
  - cases regarding child abuse images, online child abuse, grooming etc
  - **computer crime:** computer intrusion, data interference and system interference (DDoS etc), internet banking fraud

Internet investigation support

- Obtaining records from service providers
  - Mostly BSI/IP-logs
  - Also content data
- Internet investigations
  - Capturing web content as evidence
  - Identifying users
  - Locating users
- Open source intelligence
- Covert online investigations
- Emergency/urgent cases
  - G8 (24/7–network)

NCIS Norway org. chart



Norwegian legislation

The Criminal Procedure Act of 1981

- General provisions, electronic evidence not regulated specifically

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.

Internet records: 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.

Internet records: 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.

Data retention vs duty to erase data

- The EU Data Retention Directive was approved by the Norwegian Parliament in 2011 (6 months retention of phone records and IP logs), and will be implemented by July 1, 2015.
- Currently, phone records are kept by the telecoms for up to 3-5 months, and IP logs are kept by the ISPs for up to 21 days, based on billing practices and several decisions from the Norwegian Data Protection Authority and Article 28, first subsection in the Personal Data Act:

"The controller shall not store personal data longer than is necessary to carry out the purpose of processing. If the personal data shall not thereafter be stored in pursuance of the Archives Act or other legislation, they shall be erased."

Section 192: search

"If any person is with just cause suspected of an act punishable pursuant to statue by imprisonment, a search may be made of his residence, premises or ***storage place*** *in order to undertake an arrest or to look for evidence that may be seized or on which a charge may be created. (…)"*

Does this apply also to online search?

Section 203: seizure

*"**Objects** that are deemed to be significant as evidence may be seized until a legally enforcable judgement is passed. The same applies to objects that are deemed to be liable to confiscation or to a claim for surrender by an aggrieved person."*

The term "objects" include electronic evidence such as bank account information, IP logs, domain names (at least .no domains) etc.

Section 210: production order

- *"A court may order the posessor 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 decisions of the prosecution authority shall be submitted to the court for approval as soon as possible."

Section 208: information about the seizure

- *"Every person who is affected by a seizure may immediately or subsequently require the question whether it shall be ratified to be brought before a court. The prosecuting authority shall ensure that any such person shall be informed of this right."*

- Section 208a:
  "(…) the court may by order decide that (…) information (…) to the suspect or other persons affected by the seizure may be deferred if strictly necessary for the investigation of the case that such information shall not be given."

Suppression of evidence?

- Courts may suppress illegaly obtained evidence, based on case law
- Evidence obtained legally in another country, according to their laws and practices, may be used in Norway, even if it would not have been possible to obtain the evidence in Norway, according to Norwegian laws and practices:
- HR 2002-1665: evidence from phone wiretaps in Spain accepted. The wiretaps were done in Spain, in accordance with Spanish laws, by the Spanish police after requests from Norwegian police. This was not possible in Norway; the maximum penalty for the violation was too low.

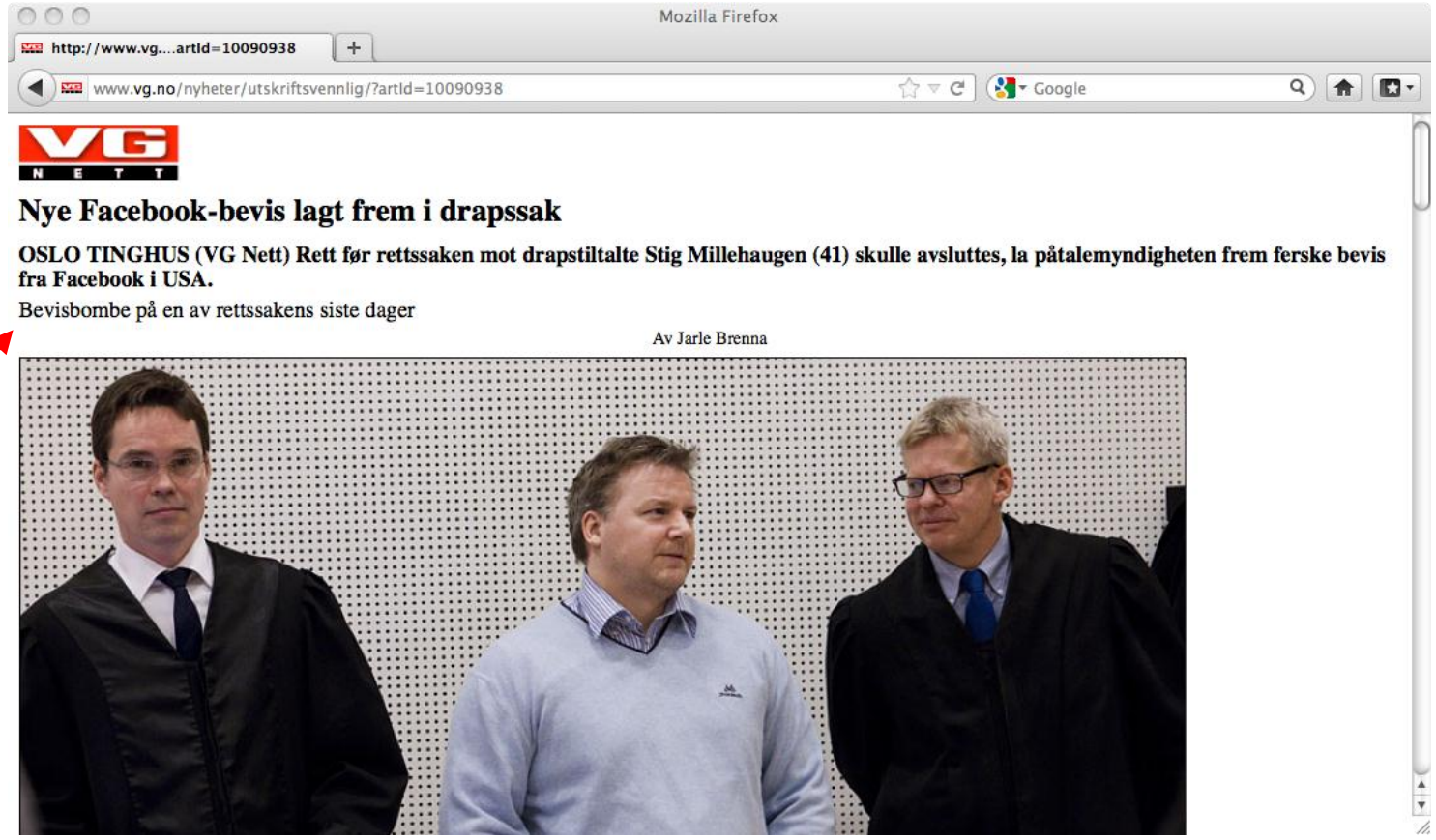
Electronic evidence and international cooperation: three case examples

- The «Haugerud» murder case
- The «Sigrid» case: missing teenager, later found dead
- ”Lost Boy”: international pedophile network

Example 1: the «Haugerud» case

- January 19, 2009: person found dead in a car at Haugerud, Oslo.
- Several parties involved connected to organized crime
- Facebook data a central part of the evidence: a fake Facebook profile used for communication between the accused, before the murder took place
- Request to Facebook based on evidence found after searches and digital forensics in Norway
- The previously available Facebook data proved that the fake profile used the IP address used by one of the accused. The Facebook data (content of messages), received one year after the request, (April 2011) during the final days of the trial proved that several statements from the accused regarding their contact before the murder, were incorrect.
- Both of the accused were convicted.

If the data had arrived a few days later?



Example 2: the «Sigrid» case

- Aug 4, 2012: 16 year old girl missing
- Possible evicence: her Facebook data, such as messages and location information
- The original request from the police in Oslo, via the 24/7 network, was based on exigent circumstances.
- What kind of data could Facebook give to the police in Norway without a court order in the U.S.?

NEWS

Facebook denies Norwegian police access to missing teen's account

By Jordan Valinsky on August 09, 2012
more articles | email

Follow @jordan327 1,206 followers

FACEBOOK — As Norwegian police search for missing 16-year-old Sigrid Schjetne, they'll have to do so without access to her Facebook account to assist them.

During a press conference Thursday, Oslo police inspector Hanne Kristin Rohde said Facebook denied their request to access Schjetne's account to help them gain insight into Schjetne's whereabouts.

However, a Facebook spokeswoman told the Daily Dot that the company does not give full access to user's accounts, but the company is working closely with Oslo police to provide as much information as possible.

RELATED STORIES


Stockholm police track lost teddy bear on Facebook

Exigent circumstances, according to Norwegian law and practices

Exigent circumstances: implied consent?

- Example: search and rescue operations.
- Typical case: people missing in the mountains or at sea, request to track their cell phones

Exigent circumstances: criminal investigations

- To stop or prevent imminent, serious criminal acts
  - Emergency: clear and present danger to life, health, property or other interests
  - The coercive measure must be a relevant and neccessary part of solving the emergency situation
  - The risk of the emergency is significantly larger than the risk connected to the actions by the police
  - No other relevant legal measures
  - Only during the emergency situation, not afterwards

Exigent circumstances: examples

- Abductions
  - The «Faiza» case, February 3, 2010: abduction victim called the police from the booth of a car.
  - Counterexample: not exigent circumstances if a divorced parent takes a child without accept from the other parent, unless there is information about specific danger for the child.
- Terrorism
- Hostage situations

Exigent circumstances:

- Exigent circumstances makes it possible to use various measures, including phone wiretaps, access to cell phone location data, IP logs and access to content data
- Generally, the deciscion will be made by the Chief of police
- Norwegian telecoms have generally accepted requests from the police and prosecutors based on excigent circumstances.
- Rarely used in Norway

Other urgent requests

- Urgent requests are handled by NCIS Norway, as the national 24/7 contact point
- The largest telecom/ISP in Norway (Telenor) has a 24/7 police response centre
- In other cases (smaller telecoms etc), urgent requests may take more time

Example 3: the ”Lost Boy” case

- The investigation started in Norway, after one complaint against a Norwegian 43 year old male:
  - A 15 year old boy met another ”teenager” via internet chat, agreed to meet ”him”, invitation to a hotel room
  - 2005/06: bought sex from young boys in Bergen, Norway, on several occasions and probably other occasions in Norway as well.
  - After his release from custody in November 2007, bought sex from several young boys in Eastern Norway.
  - His PC analysed in 2007 by computer forensics – a breakthrough:
  - Computer forensics managed to restore deleted hard-disks: e.g. chatlogs
    2426 child pornographic pictures
    140 child pornographic movies
    Several pictures of young boys posing, probably made by the perpetrator himself
    Several chatlogs concerning abduction and rape of young boys

”Lost Boy”: the Italian investigation

- Evidence showed links with perpetrators from other counties (Italy, Romania)
- Italian perpetrator: arrested in Italy in December 2007 as a result of a joint Italian/Norwegian action.
- Arrest was initiated by a Norwegian rogatory letter, which was executed in **only 14 days** with **Eurojust’s** intervention

- Results (partial) of the forensic analysis of the seized materials:
  - 1.271.496 pedopornographic images from external sources
  - 5.709 pedopornographic films from external sources
  - 19.306 self-made pedopornographic images
  - 8 self-made pedopornographic films
  - 32 hours of non-edited self-made pedopornographic films

- Forensic examinations of seized computers showed evidence of links with the perpetrators from other countries (Norway, Romania, USA, Pakistan).

”Lost Boy”: Eurojust

1.Coordination meeting at Eurojust on 17th October 2008:

- Exchange of rogatory letters and evidences between all parties involved;
- Objective in common efforts following consultations with National Authorities;
- Evidences brought personally to Washington DC by a liaison prosecutor at Eurojust, in order to start investigation;

2.Video conference at Eurojust on the 6th November 2008:

- Between Norway and the US;
- Exchange of information;
- State of play of both investigations;
- Preparation for a common action against targets identified in Los Angeles

3. Several coordination meetings as the investigation progressed, the latest at **Eurojust February 3, 2010**

”Lost Boy”: international scope

- Analysis of **IP addresses and member communications** suggested members were also located in Belgium, Brazil, Canada, France, Germany, Mexico, Netherlands, New Zealand, UK.
- US sent lead packages to above-listed countries in October 2009.
- Images suggest child victims were located worldwide (Europe, North and South America, Asia).
- Members were sending money to someone in the Philippines, possibly to produce new images.
- Second most prolific poster, screen name “Novice,” Japanese national, Canadian landed immigrant, currently detained in Los Angeles.
- One defendant was living in the Czech Republic and deported from Prague on January 6, 2010. He had previously been convicted of child pornography crimes in the USA and was a registered sex offender

”Lost Boy”:

- 35 “Lost Boy” members in total, including 15 US nationals.
- Many used proxy servers and other methods to conceal identity, but 16 were identified.
- 15 were detained in Los Angeles (2 extradited from CZ and Honduras), and faced a 20-year mandatory minimum sentence, 3 pleaded guilty – lower sentence (15 years, 5-20 years, 8-10 years)
- Some defendants were cooperating, and identifying numerous additional hands-on offenders
- Example: March 5, 2012: “Jonathon Sudduth of Springfield, Ill., was sentenced today (…) in Los Angeles to 22 years in prison and lifetime supervised release for conspiracy to advertise child pornography” (…) Todays sentencing is the result of an international investigation into the “Lost Boy” online bulletin board.” www.justice.gov/opa/pr/2012/March/12-crm-283.html
- The Norwegian suspect was sentenced to 10 years preventive detention for sexual abuse against 16 boys between 10 and 17 years old, and to pay restitution to 9 of the victims. His appeal to the Supreme Court was rejected (January 2011).

”Lost Boy”: the value of cooperation

- The results in this case would not have been possible without an efficient international cooperation
- Access to and analysis of electronic evidence, such as IP addresses, was an important part of this investigation

Norway and The Budapest Convention

Experiences with the 24/7 network and expedited preservation (art. 29)

- The number of requests for expedited preservation from Norway to other countries, is lower than the number of requests for preservation directly to international service providers (Facebook, Google, Microsoft, Skype, Yahoo…)
- But without the possibility for preservation based on the convention, it could have been more difficult to contact the service provides directly
- Typical request: logs from ISPs and/or website hosting companies.

Experiences with the 24/7 network and expedited preservation (art. 29)

- Usually a fast reply from the 24/7 contact points, still various challenges
- Jurisdiction?
- Difficulties in accessing the data in question, example: co-hosting solutions
- Deleted data?
- Uncooperative companies
- Legal challenges based on local legislation
- Securing data vs accessing data

Conclusions

- Many cases would be impossible to solve without international cooperation
- The 24/7 network and expedited preservation is valuable and important, but has some limitations and challenges
- **Most common challenge: the request comes too late**
- Using the 24/7 network to preserve data takes less time than sending a request for mutual legal assistance

eirik.tronnes.hansen@politiet.no