

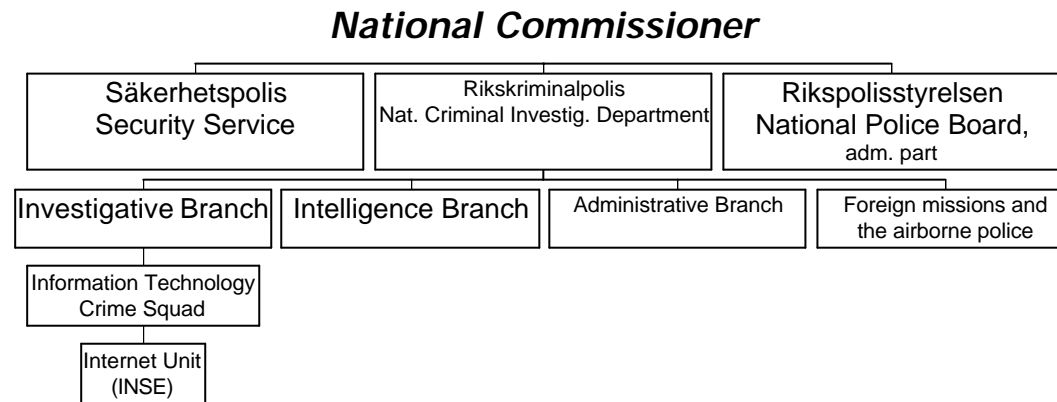
Information Technology Crime

An overview

Superintendent Stefan Kronqvist
National Criminal Investigation
Department
Information Technology Crime
Squad

2002-01-24

Brief organisational overview



Staff

- 1 Chief of Squad
- 2 Deputy Chief of Squad
- 10 investigators; 5 dealing with operational and forensic cases, 5 dealing with Internet cases
- 2 Technical advisors
- 1 clerk
- Attached personnel for various purposes

Some historical remarks of the Squad

- FBI-training 1985 and a specially designed domestic training 1986
- Operational start 1986 as a part of the NCID Economic Crime Squad)
- National Central Reference Point (Interpol NCRP) 1993
- Independent NCID unit 1995
- Squad 1998
- G 8 24/7-service since 1999
- Internet unit since 2000

Actions

- Operational support to local police departments
- International contacts
- Training
- Development of tools and techniques
- Some intelligence actions
- Internet surveillance
- Cooperation with the industry and governmental authorities
- Hub for a domestic point-of-contact police network

Case flow

- 1998: appr. 300 cases
- 1999: appr. 320 cases
- 2000: 333 cases; investigations, intelligence actions and support to foreign LE agencies
- Most frequent crime 1998: Aggravated purchasing of drugs, 1999: Serious crimes against life and health
- 2001: 349 cases

International work

- Interpol European Working Group On Information Technology and Crime - medverkan since 1993
- IOCE - International Organisation On Computer Evidence (Forensics)
- Cooperation with FBI, CRI m.fl.
- NCRP - Interpol and G 8
- Europol (High Tech Crimes linked to organised crimes)
- Nordic cooperation
- Swedish EU- Presidency 2001
- The Commission's Action Plan against Cybercrime

The Cybercrime Convention

- Initiative from Council of Europe
- Will –hopefully- be adopted november 2001
- Will give crossborder investigations more power
- Will impliment European standards

Training

- Regional meetings
- Seminars
- Basic and advanced training:
- 12 weeks basic training
- 3 weeks advanced training



Our way to do it...

- House search and support to search teams
- Analysis of seized items and data storage media (Forensics)
- Tracing and identifying of suspected persons in Cyberspace
- Advises
- Technical support to various actions



INSE (Internet unit)

- Established dec 2000
- Initial phase 2001:
 - Tasks, needs and limits
 - Legal study on some cybercrime issues
 - Technical project
 - Recruitment

Other Swedish IT-crime units

- Available at some local PD
- EBM (Serious Economic Crime Bureau)
- SKL (National Forensic Laboratory)

Crimes we deal with

- All traditional crimes but IT-specialized investigative skill is an absolute need for success
- Economic Crimes
- Internet fraud, e-commerce fraud
- Computer and system intrusions
- Espionage
- Violation of Intellectual Property Rights
- Illegal internet commerce; prostitution, drugs, restricted medicines etc
- Sexual abuse of minors

Examples of offences

- Software piracy; distribution via CD-ROM or the Internet, production centrals can be almost "industrial"
- Purchasing of various counterfeited items via the Internet
- Purchasing of parallel production; medicines etc via the Internet
- Illegal distribution of material protected by copyrights; novels, pictures, music etc, etc via the Internet
- Crossborder investigative problems

Basis of investigation

- Cooperation with the victim is important
- Only the victim knows all details of his/her/their rights
- Concerning software piracy, facilities from the victim could be necessary
- An investigative strategy should be considered by the prosecutor and the police investigators (What do we need, must all seized material be examined?)

Manuals 1.

- Manuals are not a solution, only a support
- Manuals can not replace skill or experience
- Manuals are not law, only guidelines
- BUT..
- Manuals are based on approved methods
- Manuals decreases international investigative problems
- Manuals match some irrelevant discussions in court

Manuals 2.

- Available international manuals on IT-related investigations:
 1. Computers and Crime, Interpol. Available at every NCB. Currently updated.
 2. Good practice for search and seizure in an IT-environment. Police Cooperation Working Group, European Council. Not yet finally adopted, but available for interested parties.

Good Practice

Main Chapters of the Manual

- 3 alternative methods to secure digital evidence
 1. There are plans to seize computers
 2. There are no plans to seize the hardware, evidence are secured through "mirroring" on location
 3. There are no plans to seize the hardware or to make total mirroring on location; evidence are secured through selective copying

Good Practice

Main Chapters of the Manual

- Before the search
- During the search
- After the search

Pocket Guide

- Appendix to Good Practice Manual
- "What all officers need to know"

Trends

- Organised Crime gang use IT-professionals
- Quick profit creates a new group of criminals
- Common use of encryption
- Illegal intelligence of individuals for criminal purposes

Statistics

- No particular statistics for IT-crime except computer intrusion and computer fraud.
- Report from National Audit Authority 1997 (95-96)
- Report from National Council for Crime Prevention 2000 (97-98)

Future

- The Broadband environment concentrates important system information on a local level= new points for attacks
- Traditional commerce and cash will be replaced by e-commerce and e-cash= less armed robberies but more intrusions

Movie Time

1. House search in a Bulletin Board System-environment
2. House search in an extremely complicated technical environment
3. Industrial piracy production of software