Presentation
Digital Investigations Group
(Groep Digitaal Rechercheren)
We fight Cybercrime

- Broadly defined vs narrowly defined: Old crimes, new tools vs new crimes, new tools

- ICT has either been used as a tool when a crime has been committed or

- ICT is actually the specific target of a criminal act
A brief history

- 1995: more cooperation between intelligence units and technical experts within the KLPD due to the upcoming of a new technology as well as a new economy

- 1998: complaints from internet users as well as political pressure concerning the presence of images containing child pornography on the net result in the formation of a special task force targeted at apprehending those who manufacture or distribute those images
• 1999: The KLPD decides to combine all computer crime fighting efforts into one task force

• Parties involved agree to a pilot phase of 1 year
Successful projects such as

- SKIM (Child pornography on the Internet),
- Euro2000i (Hooliganism),
- DNBi (Financial fraud using private chatrooms)

as well as the fact that the technical support and advice of the cybercops with regard to other police investigations proved very successful, led to the continuation of the pilot with again 1 year up until October 2001.

Early 2001 the cybercrime fighting team expands from 9 to 23 employees.
• Mid 2001 the KLPD was convinced that it was time to end the pilot phase and to add this task force to one of her twelve Special Services, hereby embedding the team into her ‘product line’

• This means that as of last year the Cybercops are officially part of the Criminal Investigation Service (Dienst Recherche Onderzoeken) of the KLPD!
The Digital Investigations Group is made up of four teams of specialists

1. **The Advisers**: policy-making and consultancy with regard to the fight against cybercrime. Cooperate with local police forces, the Public prosecutions Department, the Ministry of Justice as well as the Ministry of the Interior

2. **The Internet Investigators**: ‘patrolling’ the Internet and tracking down suspects of Cybercrime
3. **The Digital Investigators**: provide technical support when a search of premises is conducted. Data retrieval from computersystems and computer networks as well as data analysis

4. **Research & Development**: ICT specialists develop customized tools and techniques which investigators use in the combat against Cybercrime
In summary,

• we track down suspects of Cybercrime,

• we develop the tools to do it,

• we tell others how we actually did it and

• we help them out with their investigations in case they do not yet have the necessary means or know-how
The types and varieties of Cybercrime we encounter in the Netherlands
Cybercrime

- Hacking
- Handling stolen goods
- Drugs trade on Internet
- Construction fraud
- Marriage Maxima & Willem Alexander
- Child pornography on Internet
- Data Interception
- Illegal medicine trade
- Assassination of Pim Fortuyn
- Threat / duress

- Graffiti on trains
- Counterfeiting
- Defacing
- 0900 Fraud
- Introduction €
- Extortion
- Viruses & Trojans
- Terrorism
- Fake IDs
- Infiltration methods
- DoS attacks

Priority?
Although we try to set priorities, major events like

- The terrorist attacks in the US
- Large-scale construction fraud in the Netherlands
- The assassination of Pim Fortuyn

make that extremely difficult
From Januari 2001 up until July 2002 we have dealt with 348 cases* of Cybercrime. This is our present Cybercrime TOP TEN LIST

1.   Terrorism (55)
2.   Fraud (44)
3.   Child pornography (34)
4.   Acts contrary to public order (32)
5.   Hacking (also defacing and DoS attacks) (29)
6.   Property crime (24)
7.   Murder cases (23)
8.   Extortion (also threat and defamation (18)
9.   Drugs trade (15)
10.  Viruses (8)

(*) This does not represent the total number of incidents that have been reported to us. Many cases are being referred on to our partners. Requests for technical support and / or consultancy are also not reflected herein.
The following topics deserve special attention

1. Legal issues
2. Cybercrime knows no borders
3. Cooperation with ISPs / Telecom Industry
4. One doesn’t know everything (call in experts)
5. Be anonymous & use the appropriate tools
6. The importance of a broad scope as well as specialization
7. Share your (technical) knowledge / expertise
8. Awareness & Education
Thank you for your attention!

Digital Investigations Group

KLPD