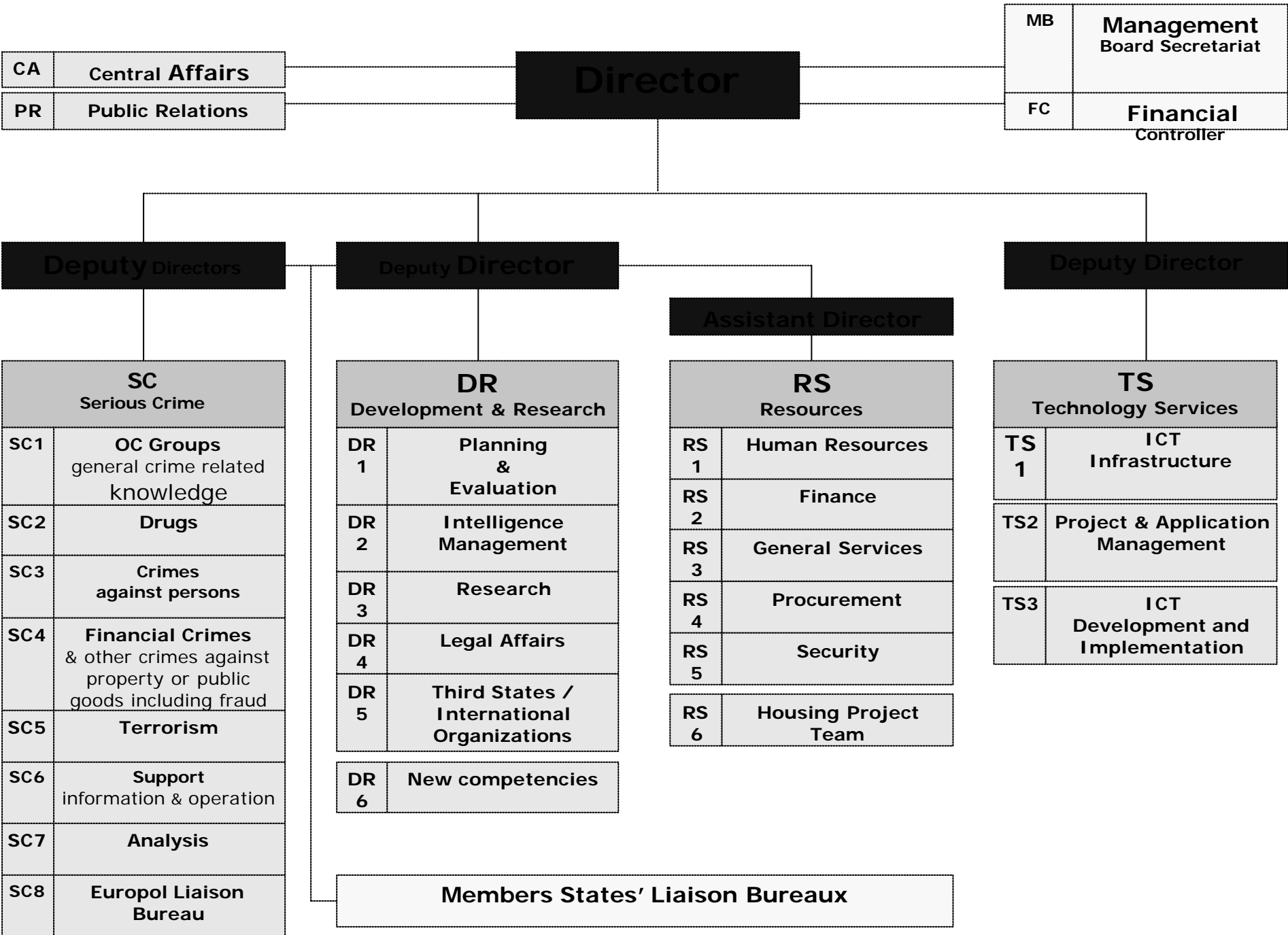




Europool



Europol



Intelligence **led** Policing



Intelligence

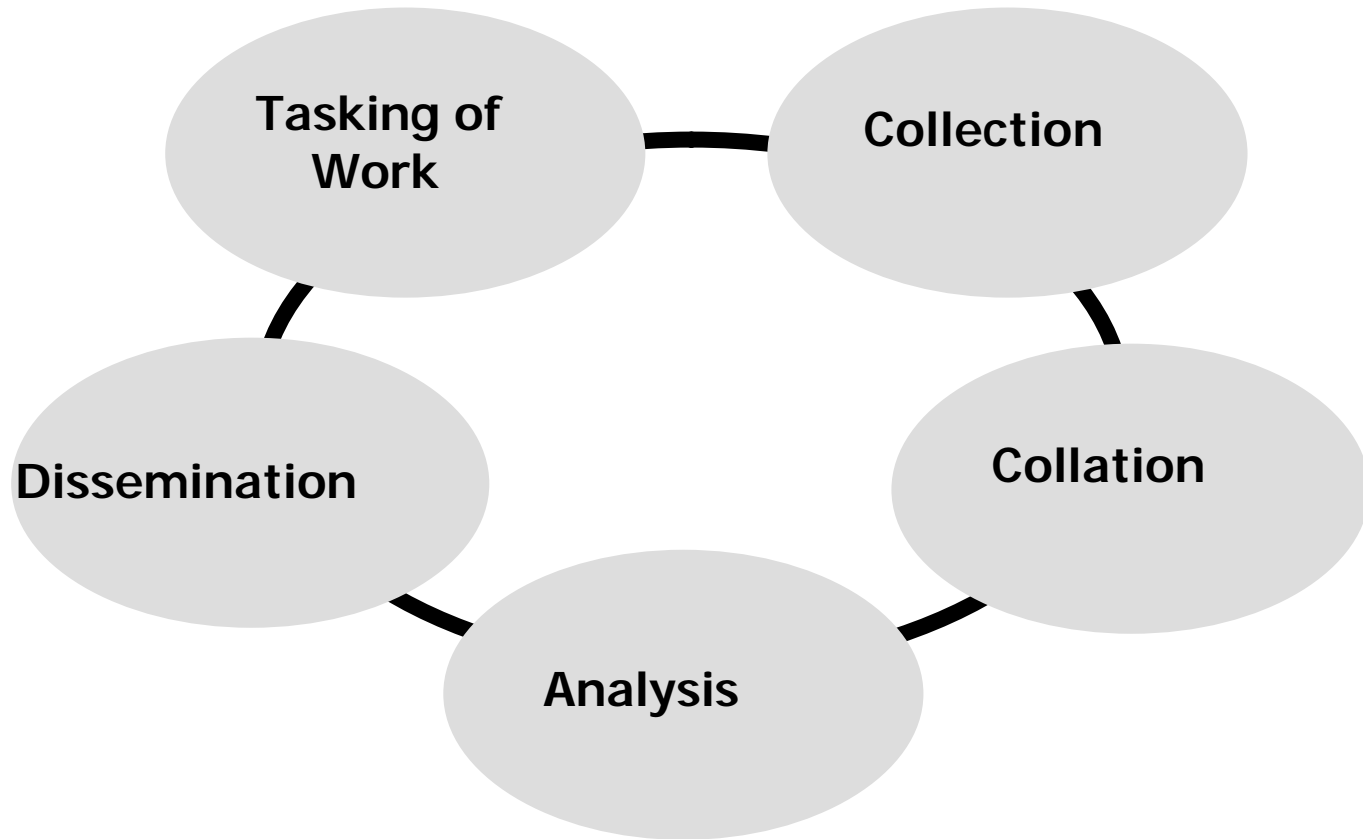
Intelligence Needs



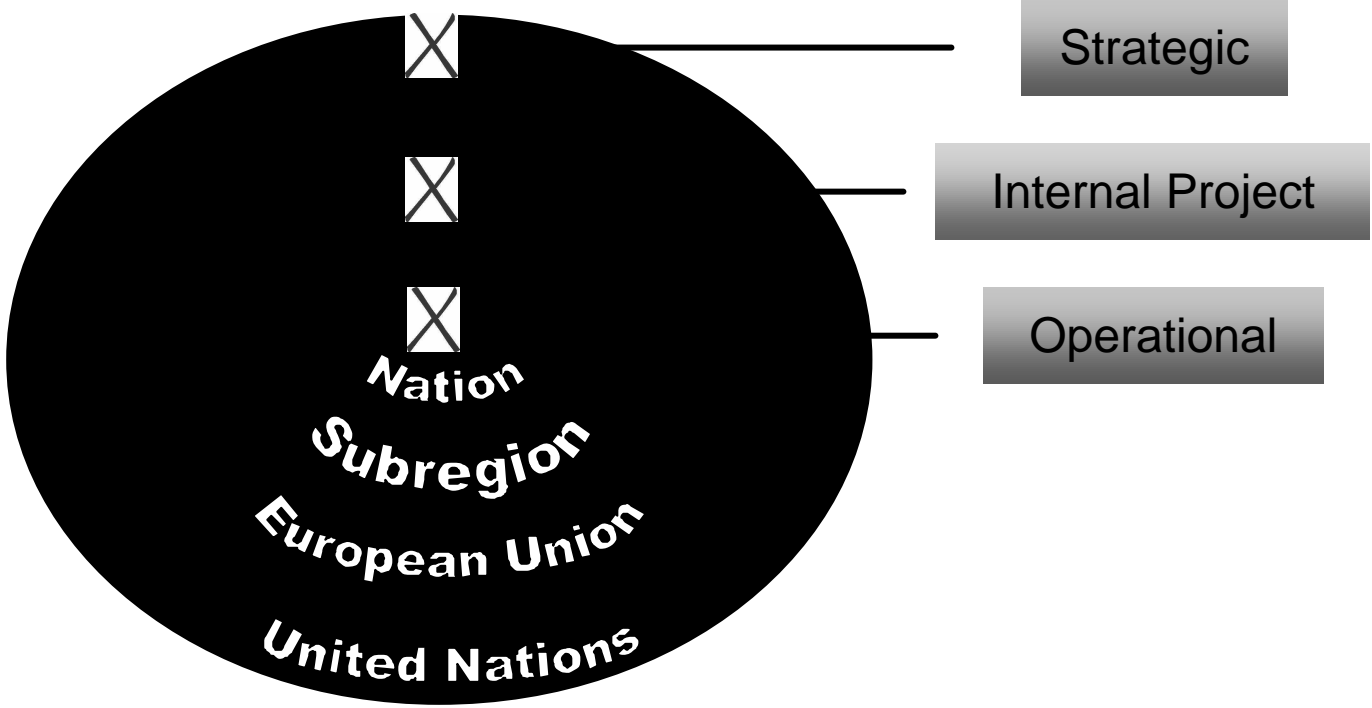
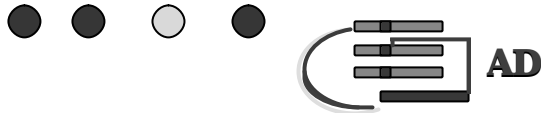
Geopolitical Aspect

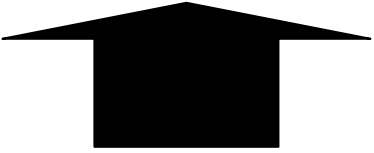
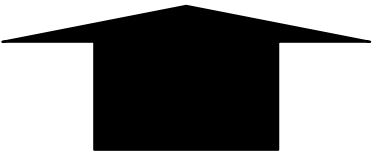
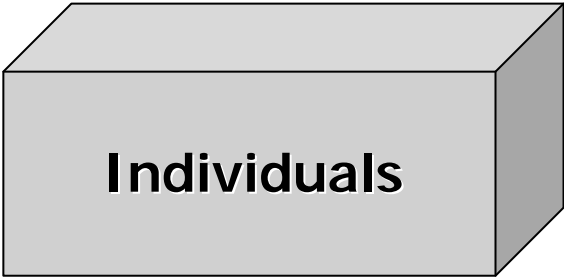
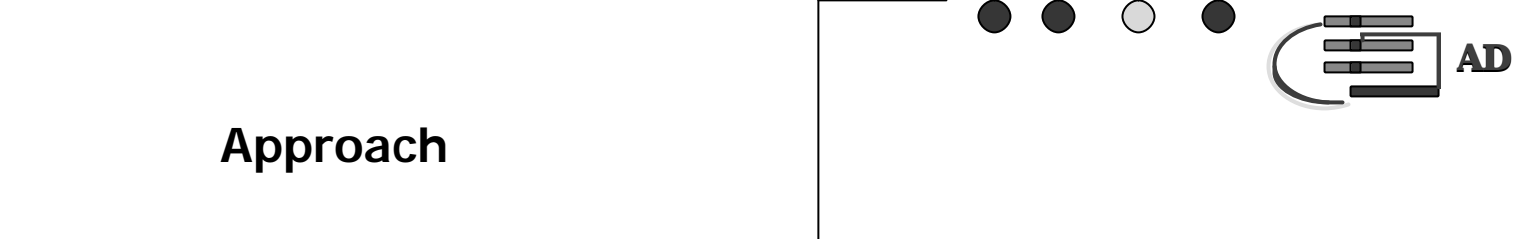


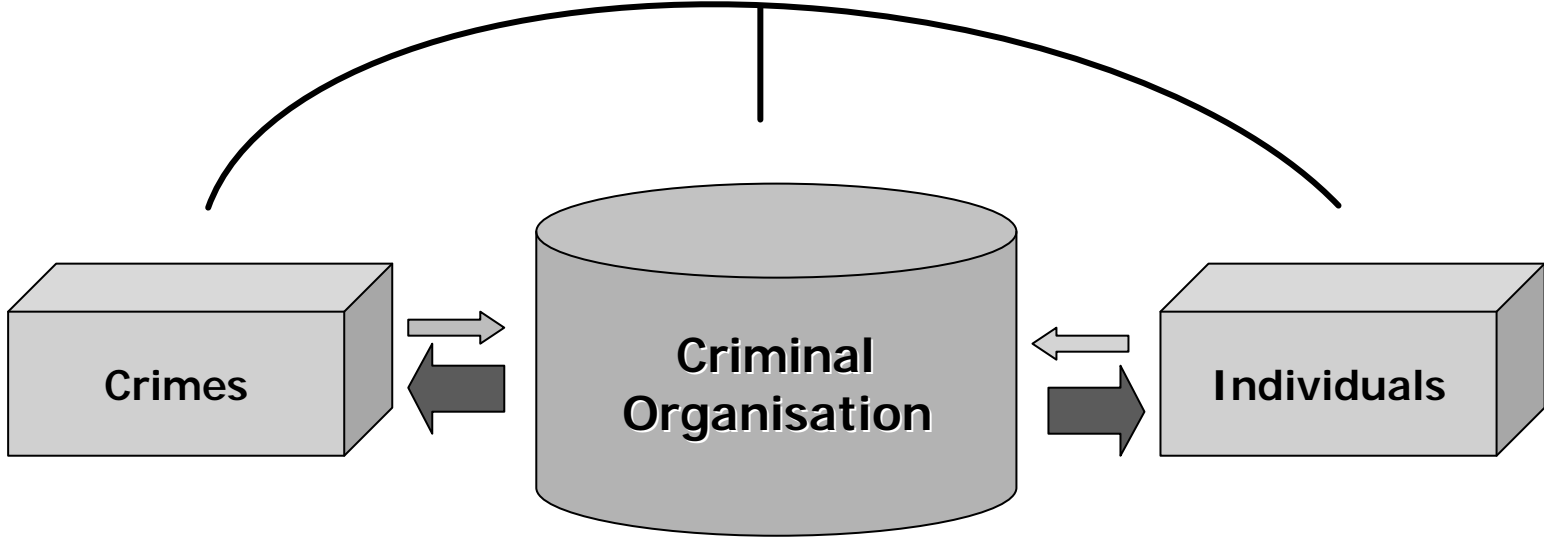
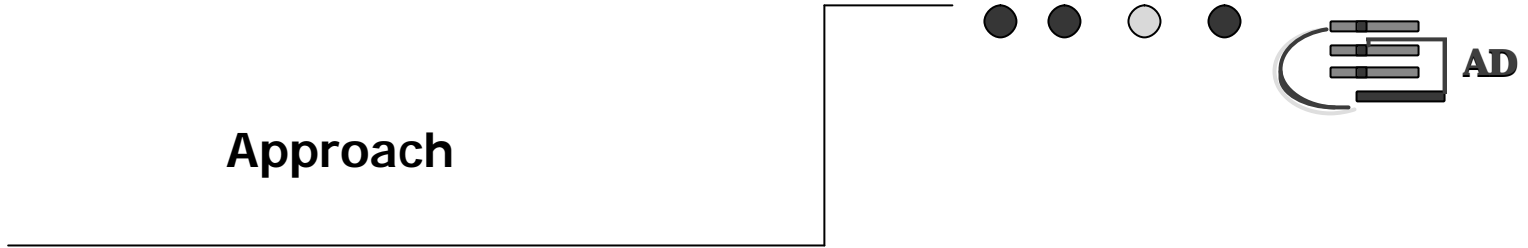
Intelligence Cycle

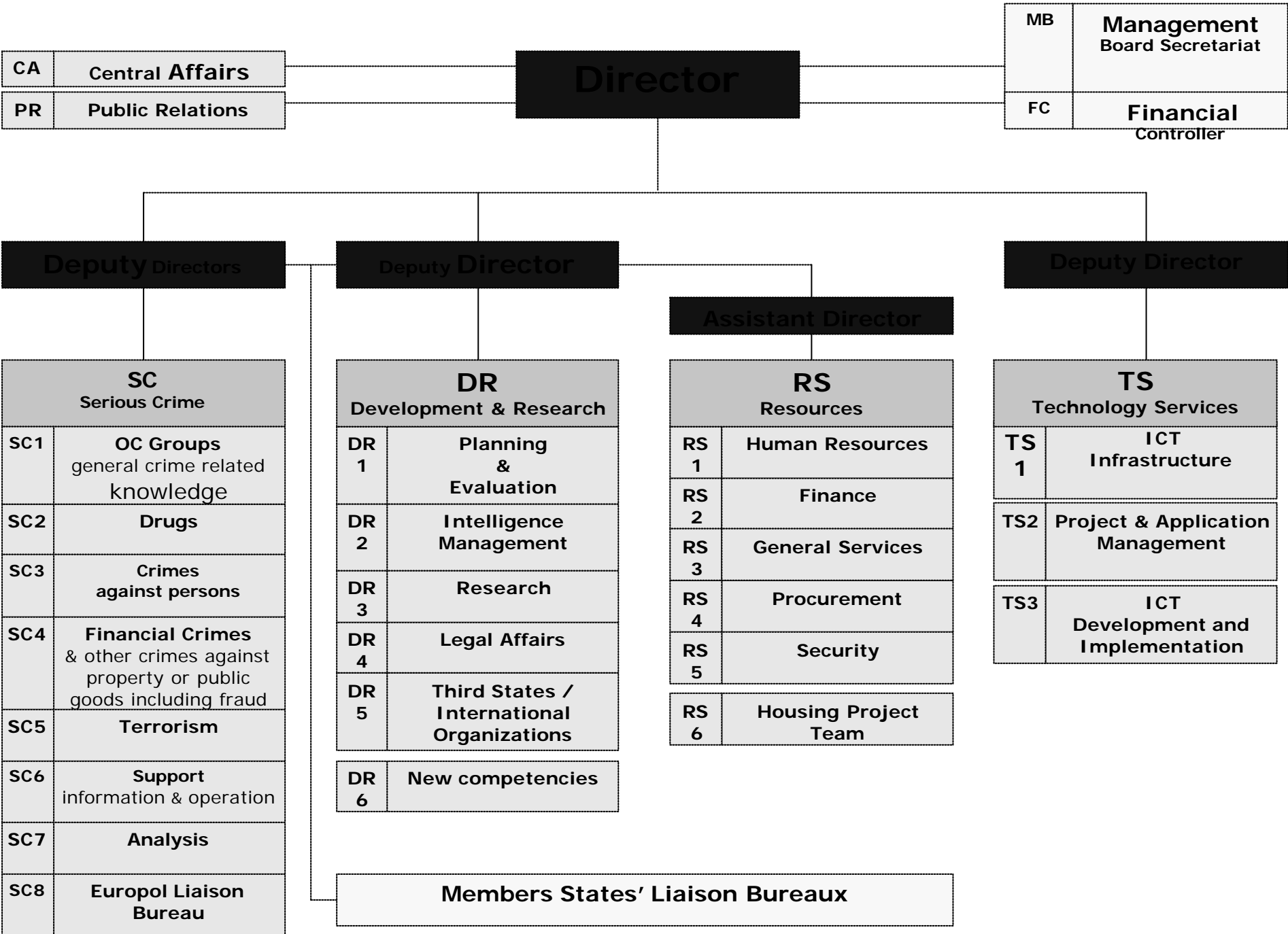


Geopolitical Aspect

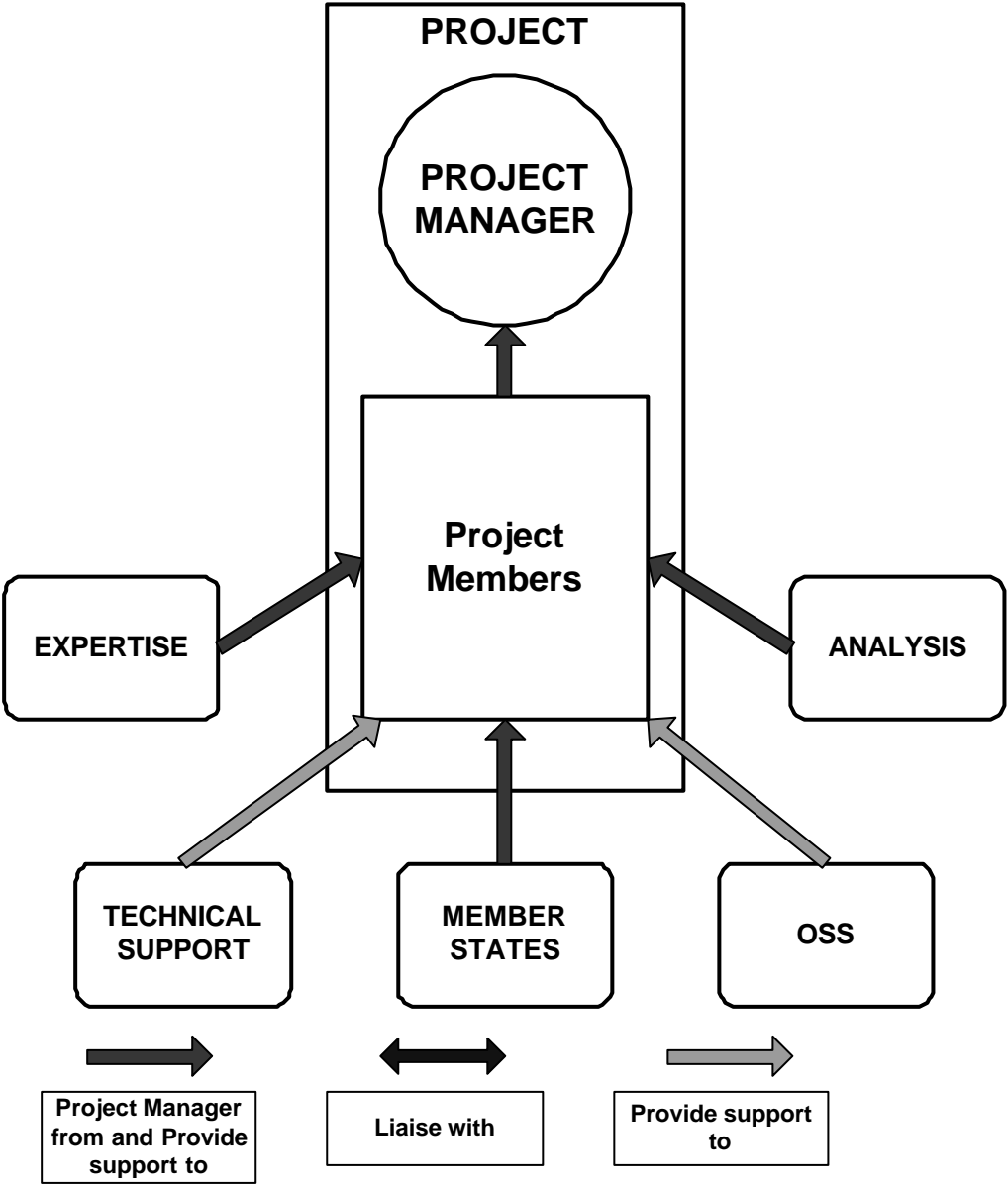
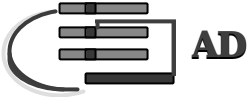
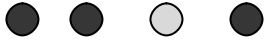




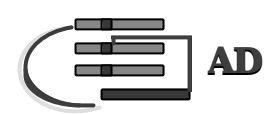




Team Work Concept



Intelligence Products



strategic products

- Threat Assessment
- Risk Assessment
- Situation Report
- Intelligence Bulletin
- Policy Report

operational products

- Criminal Organisations
- Modus operandi
- Investigation Support
- Operational Support
- Technical Support

Cyber Crime?
Digital Crime? High-Tech -
Internet crime?



The problem

- **The complex and trans-national dimensions**
- **The grow of cyber crime on the Internet, not only new crimes**
- **Established crime, as illegal drug trafficking, terrorism, financial crimes, child pornography and other serious crimes**
- **Hacking as such**
- **The Member States various and different approaches**

Aims and Objectives

- **On drugs and terrorism, monitoring information flow and gathering useful information from the internet**
- **On financial crimes, to stop and/or monitor the preparation of crimes in e-commerce and money laundering via the Internet**
- **On child pornography, to facilitate the combating and dismantling of Child molesters and paedophiles networks**
- **To support cyber-investigators in sharing professional experience on-line**
- **To reduce duplication of efforts made in and between Member States.**
- **To ensure effective Law Enforcement in countering of cyber crime.**

Roles and tasks of the HTC on Cyber Crime:



- **In general the HTC should be an operational body for co-ordinating, collecting and analysing information on cyber crime**
- **The intelligence results on criminal activities**
- **Support on ongoing investigations**
- **Initiate new criminal activities**

Priority:

Due to a positive operational results which has been already achieved in the area of child pornography the Centre will start its co-ordination in the following functions:

- Establishment of a Virtual Private Network (VPN)
- Co-ordination
- Intelligence/Analysis/Risk and Treat Assessment/Development of Strategies and Actions
- Pro-active Information Collection
- Research, Development and training

Virtual Private Network



The main needs are:

- To share experiences and best practices
- Create awareness for cyber crime investigations
- Learning-by-doing
- Setup a central server for a secure communication
- Cyber crime investigators share their experiences

Intelligence products



The HTC is intended to provide investigators with integrated and structured intelligence from all sources and parties involved, focussing on:

- **Description of criminal networks and organisations**
- **Criminal roles and activities**
- **Identification of links between criminals and criminal activities**
- **Analysis of information gaps**

Pro-active approach



For intelligence use, visible online activities need to be included in the process. Based on profiles, known collected data which can be contributed - about and to:

- Targets / Criminals
- Identified new crimes
- To Member states which do not have a HTC
- To overcome language barriers (EG -> Arabic)

Research and Development

The HTC intended to actively gathering information and development about:

- **New technologies and products for Law Enforcement**
- **Investigation and prosecution methods**
- **Digital evidence examination procedures and good practice**
- **New criminal techniques and patterns**
- **Multilingual information processing, information retrieval and fact extraction**
- **Training requirements**

Co-ordination



- To reduce duplication of efforts
- To ensure effective Law Enforcement in the fight against cyber crime
- To be the substitute for those Member States without an HTC function

Work and Methods:



Based on Member States needs and experiences the operational function will focus on:

Working methods



- Identifying Member States involved in similar investigations
- Organizing operational meetings with the Member States concerned
- Establishing and guaranteeing a common strategy in cyber crime investigations
- Establishing information channels
- Maintaining ongoing analysis and dissemination of intelligence

Working methods



- Establishing and maintaining lists or data bases for intelligence and operational purposes
- Disseminating information to facilitate EU-wide and international operative activities
- Collecting and providing expertise
- Monitoring technological developments and disseminating information on ongoing research and new products to the Member States
- Establishing and maintaining contacts with the specialised units of the competent authorities

Working methods



- To identifying training needs and co-ordinating courses and training programs
- Setting up alarm procedures and acting as a full operational crisis centre for internet security
- Being a contact point for private industry at EU level using a multi-agency partnership approach.

Europol



Thank you for your attention

Questions ??

Mogens Lundh

Head of Unit, Serious Crime Department

Tel. 0031 70 30 25 121

E-mail: lundhm@europol.eu.int