### OUTLINE OF NEW DUTCH INTERCEPTION FRAMEWORK (WIV)

## Collection (1)

### Activities

The collection (receiving, taking over, storing and making accessible) of bulk-communication

Technical exploration to determine potential relevance to interception.

Crypto and malware investigation.

### **Safeguards**

**Establishing** 

intelligence

annual plans

needs /

Approval from relevant Minister.
Approval must be purpose-oriented (bound to investigation) and include proportionality, subsidiarity and necessity.

Time-limited (tbd; max 1 year).

Explicit retention periods and destruction periods.

Separation of jobs and duties; data access compartimentalization separate from data content processing.

# Preprocessing (2)/Processing (3)

#### **Activities**

Enriching and correlating data (including metadata analysis) in order to identify characteristics, identities and keywords for use in Art. 27-3 power (SIGINT selection).

Identifying and technically investigating unknown cyber threats to increase resilience.

Filtering out non-relevant data.

# **Safeguards**

Approval from Minister concerning exploration of the communication purpose-oriented, and including proportionality, subsidiarity and necessity.

Separation of jobs and duties; data access compartimentalization separate from data content processing.

Retention periods and destruction periodes for non-relevant data (tbd).

### **Activities**

Subject-oriented investigation including specific threats (eg IEDs in mission areas, cyber attacks) on the basis of the result of selected data.

Metadata analysis.

#### **Safeguards**

Approval from the Minister for selection of these data, aimed at specific individuals, organizations and technical characteristics, or keywords related to specific topics (Art. 27-3), purpose-oriented, and including proportionality, subsidiarity and necessity.

Time limit for selection (Art 27-3) (tbd; max 1 year)

Retention periods and destruction periods for unselected data (tbd).

### **Analysis**

#### **Activities**

General, subject- and threatoriented investigation; combined processing and analysis of sigint-cyber products using yields from other special intelligence means.

# **Safeguards**

Strictly speaking, this is no longer part of the interception process. It involves the use of special powers (Art. 17, 20, 21, 23, 24, 25, 28, 29) and appicable safeguards and approval regimes

t

Provisioning to intelligence consumers

WARNING: unofficial translation. Original document (in Dutch): http://www.rijksoverheid.nl/documenten-en-publicaties/brieven/2014/11/21/diagram-interceptiestelsel.html