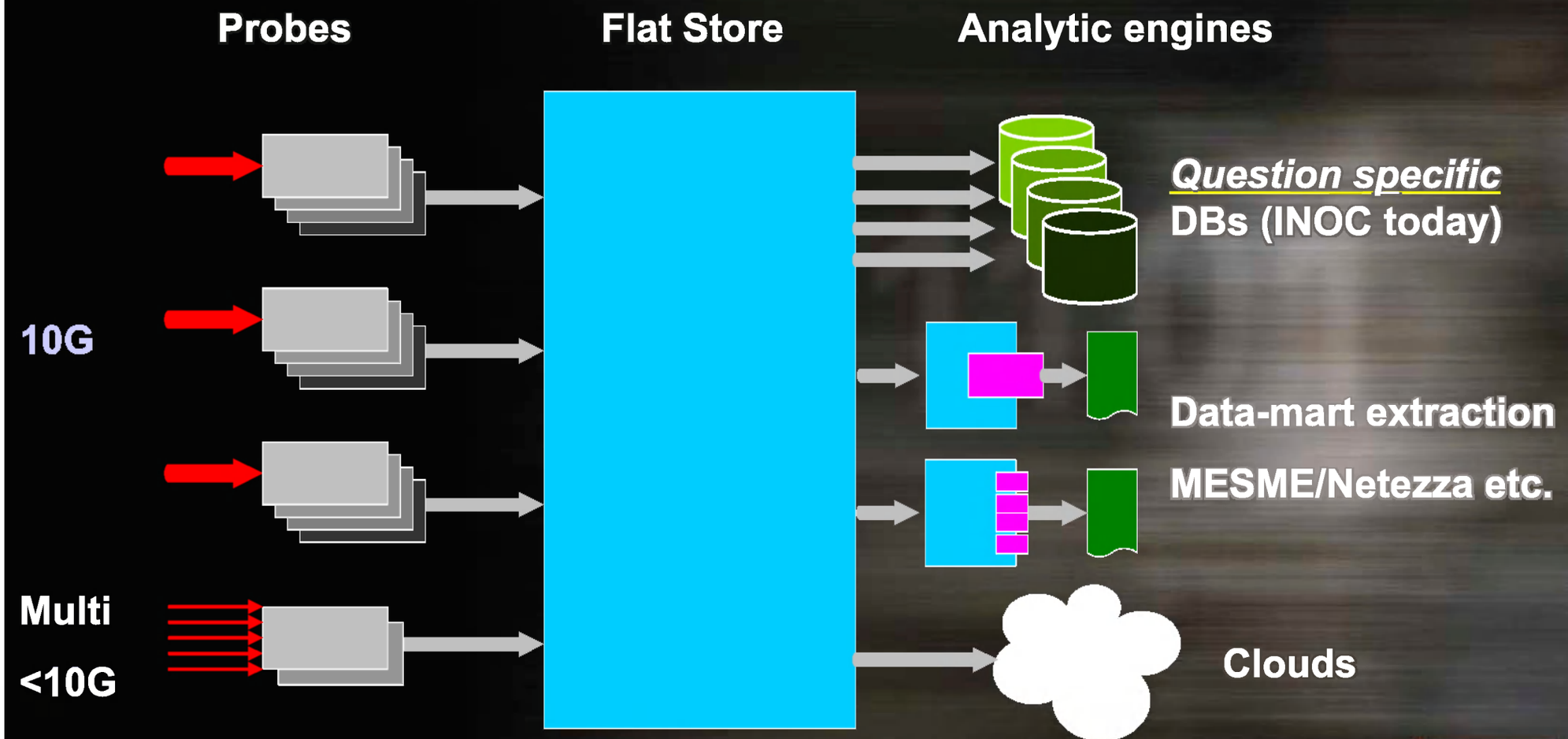
QFDs and BLACHOLE
Technology behind GCHQ/INOC

[redacted]

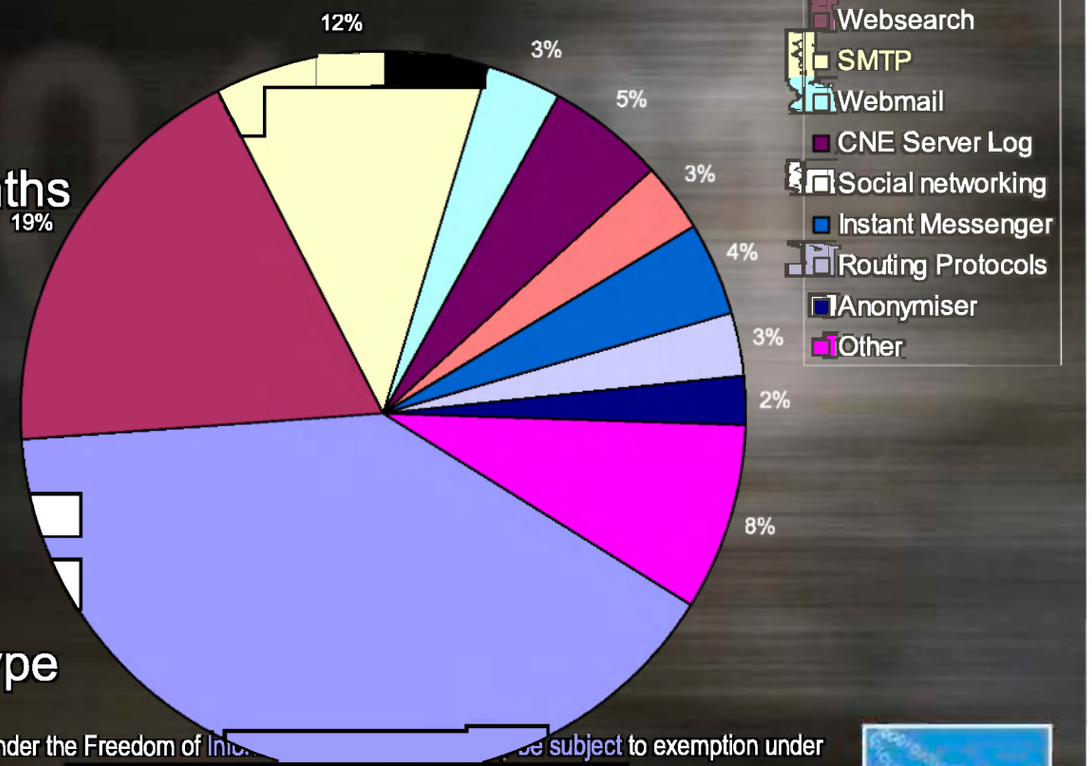
March 2009

'BLACK HOLE'



BLACK HOLE

- Flat data store – not a database
- ~ 1,100,000,000,000 events since 6th August 2007
  - 53.3TB compressed
  - 217TB uncompressed
  - 47% of data is from last 3 months
- ~10 Billion events per day
- Cheap system:
  - £1k per TB of storage
  - £20k per 10Gbps probe
  - ~£400k for 10x10Gbps prototype



Questions – INOC Today

Who, Where, When, What? – Online presence (TDI)

MUTANT BROTH

Who, which website(s)? – Online browsing activity

KARMA POLICE

Who, which fora?– Bulletin board usage

INFINITE MONKEYS

Where? – Google maps/earth usage

MARBLED GECKO

Questions – INOC Today

Who, Where, When, What? – Online presence (TDI)

MUTANT BROTH

Who, which website(s)? – Online browsing activity

KARMA POLICE

Who, which fora?– Bulletin board usage

INFINITE MONKEYS

Where? – Google maps/earth usage

MARBLED GECKO

… And many more

Questions – INOC Today

Too many specific questions… Too much for analysts to learn.

Need analyst systems to be simple and intuitive.

Let analysts find & simply understand their targets easily…

drill in to systems only when they need to

AR Prototypes - EPR Stats - Feb 2008 - Jan 2009