

APPLIED RESEARCH

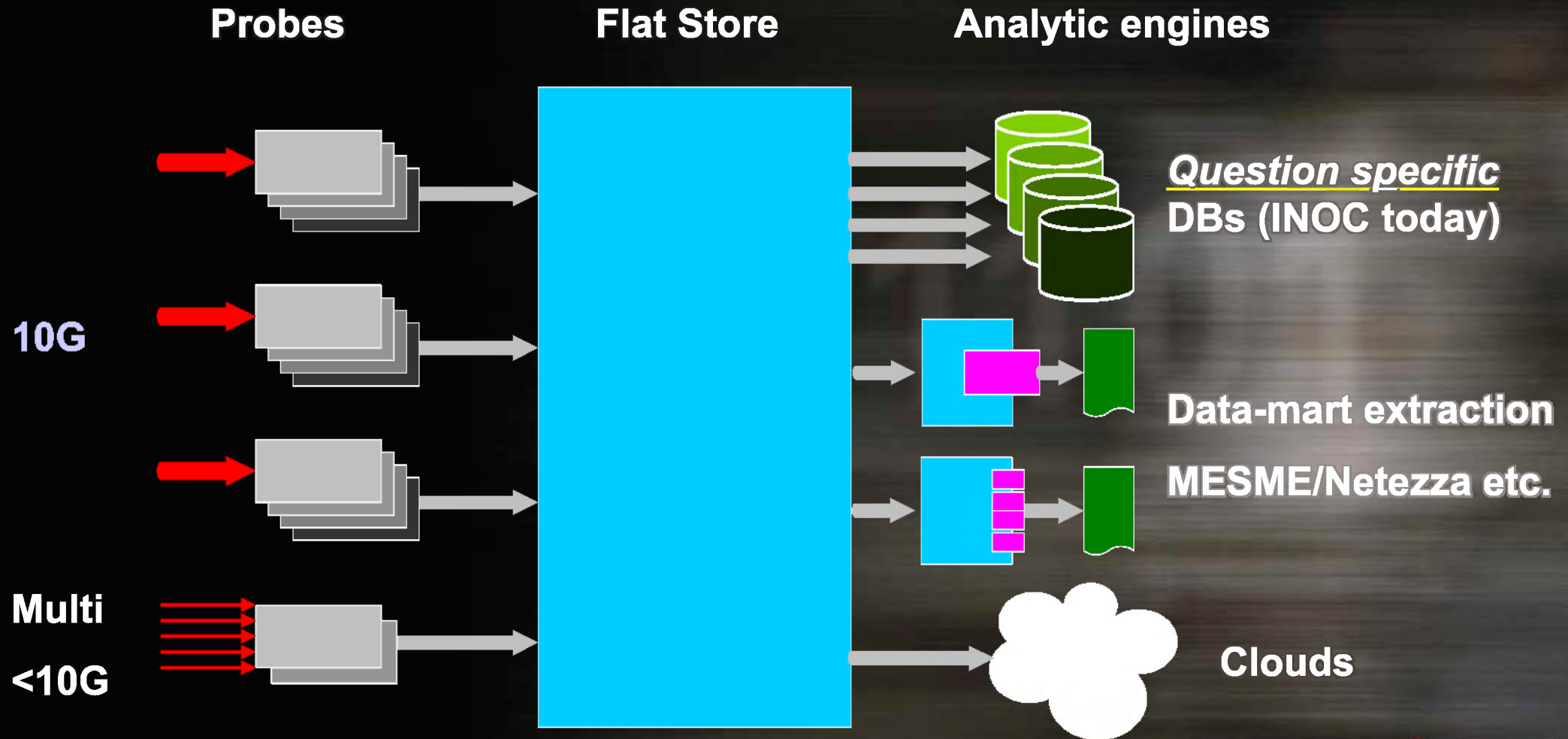
**QFDs and BLACHOLE  
Technology behind GCHQ/INOC**

[Redacted]

March 2009



# 'BLACK HOLE'

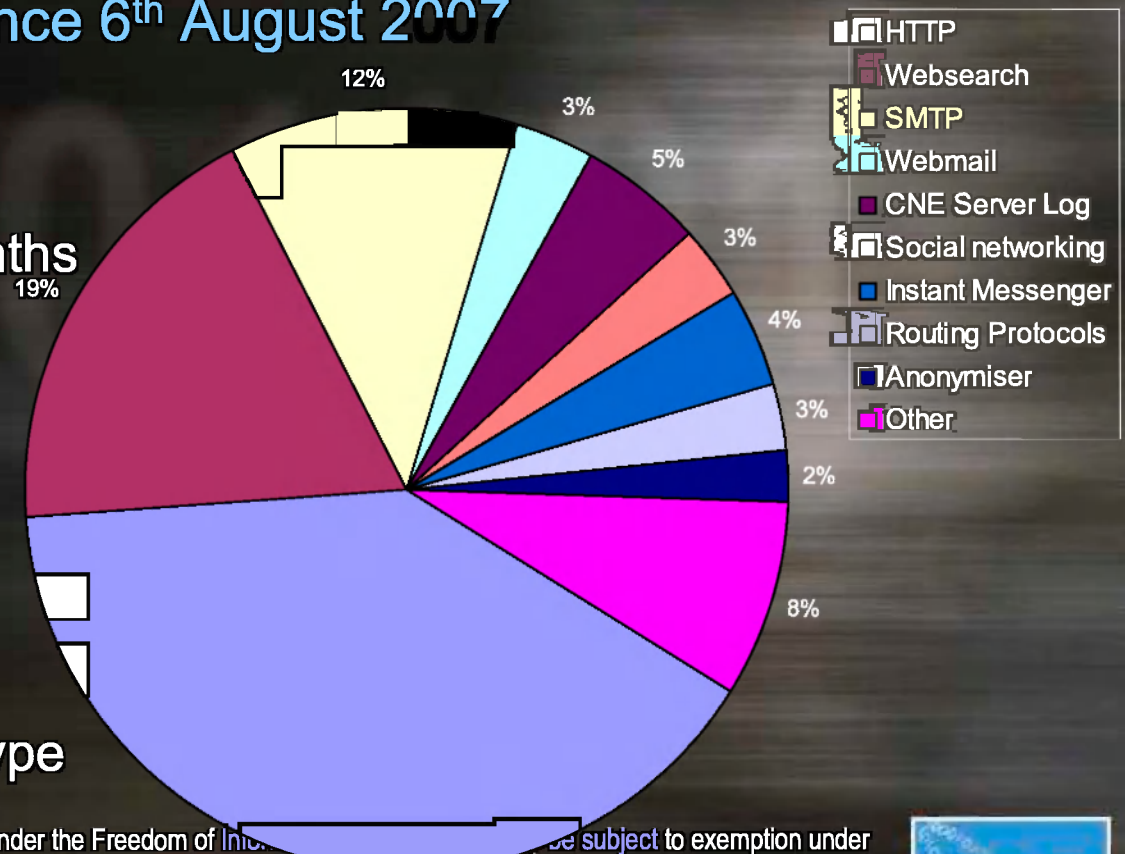


© Crown Copyright. All rights reserved. This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation. Refer disclosure requests to GCHQ on [redacted]  
Contains Intellectual Property owned and/or managed by GCHQ. The material may be disseminated throughout the recipient organisation, but GCHQ permission must be obtained for dissemination outside the organisation.



# BLACK HOLE

- Flat data store – not a database
- ~ 1,100,000,000,000 events since 6<sup>th</sup> 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



© Crown Copyright. All rights reserved. This information is exempt from disclosure under the Freedom of Information Act 2000, but may be subject to exemption under other UK information legislation. Refer disclosure requests to GCHQ on [redacted]. Contains Intellectual Property owned and/or managed by GCHQ. The material may be disseminated throughout the recipient organisation, but GCHQ permission must be obtained for dissemination outside the organisation.



# 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**

© Crown Copyright reserved. This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation. Refer disclosure requests to GCHQ on [redacted]

Contains Intellectual Property owned and/or managed by GCHQ. The material may be disseminated throughout the recipient organisation, but GCHQ permission must be obtained for dissemination outside the organisation.



# 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



**MARBL ED GECKO**

... And many more

© Crown Copyright reserved. This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation. Refer disclosure requests to GCHQ on [redacted]

Contains Intellectual Property owned and/or managed by GCHQ. The material may be disseminated throughout the recipient organisation, but GCHQ permission must be obtained for dissemination outside the organisation.



# Questions – INOC Today

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

Need analyst systems to be **simple** and **intuitive**.



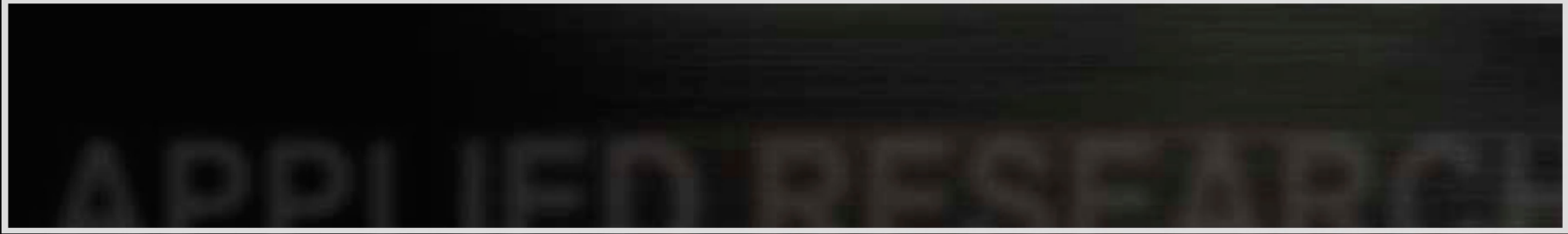
Let analysts find & simply understand their targets easily...

drill in to systems only when they need to

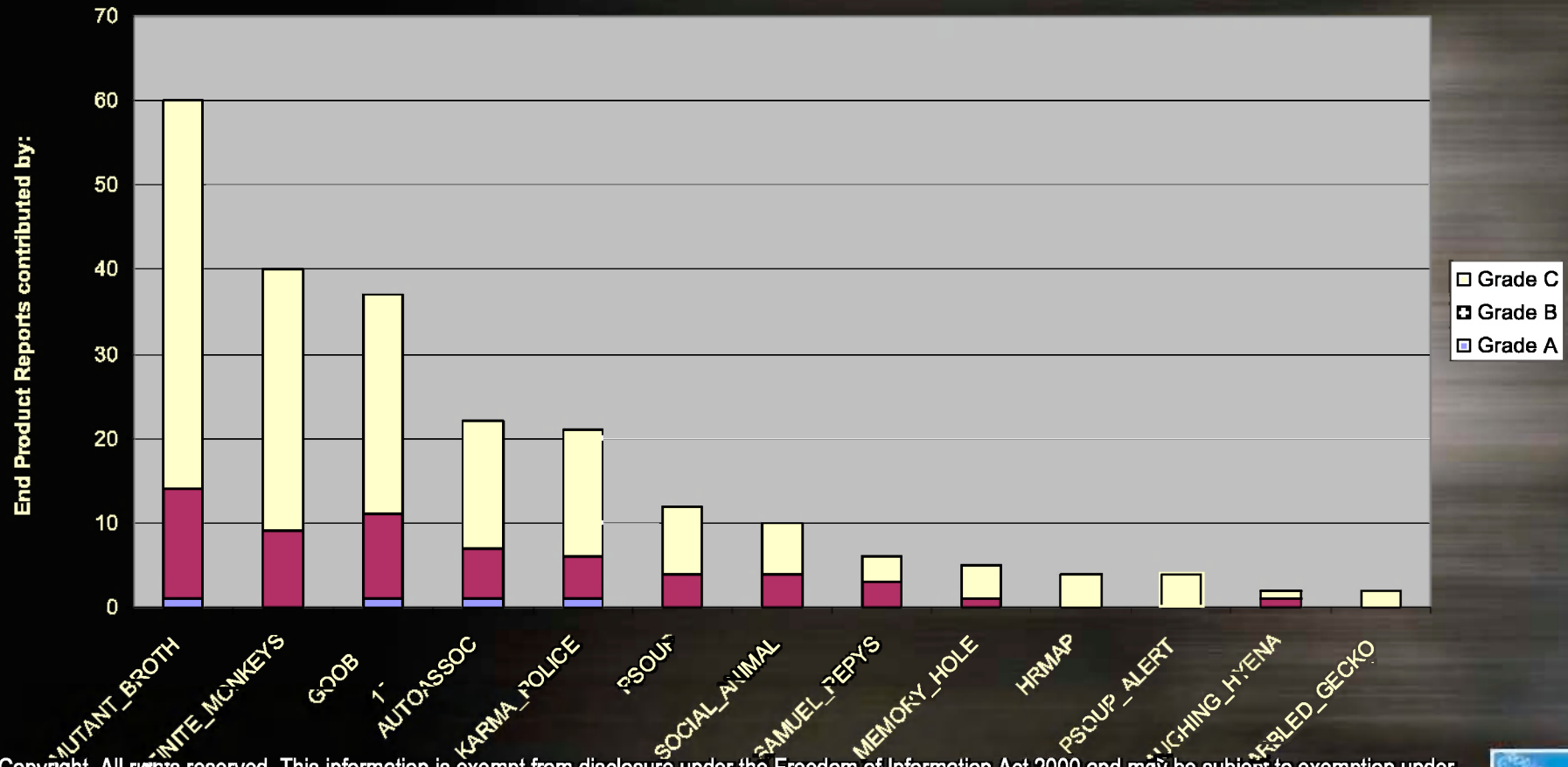
© Crown Copyright. All rights reserved. This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation. Refer disclosure requests to GCHQ on [redacted]

Contains Intellectual Property owned and/or managed by GCHQ. The material may be disseminated throughout the recipient organisation, but GCHQ permission must be obtained for dissemination outside the organisation.





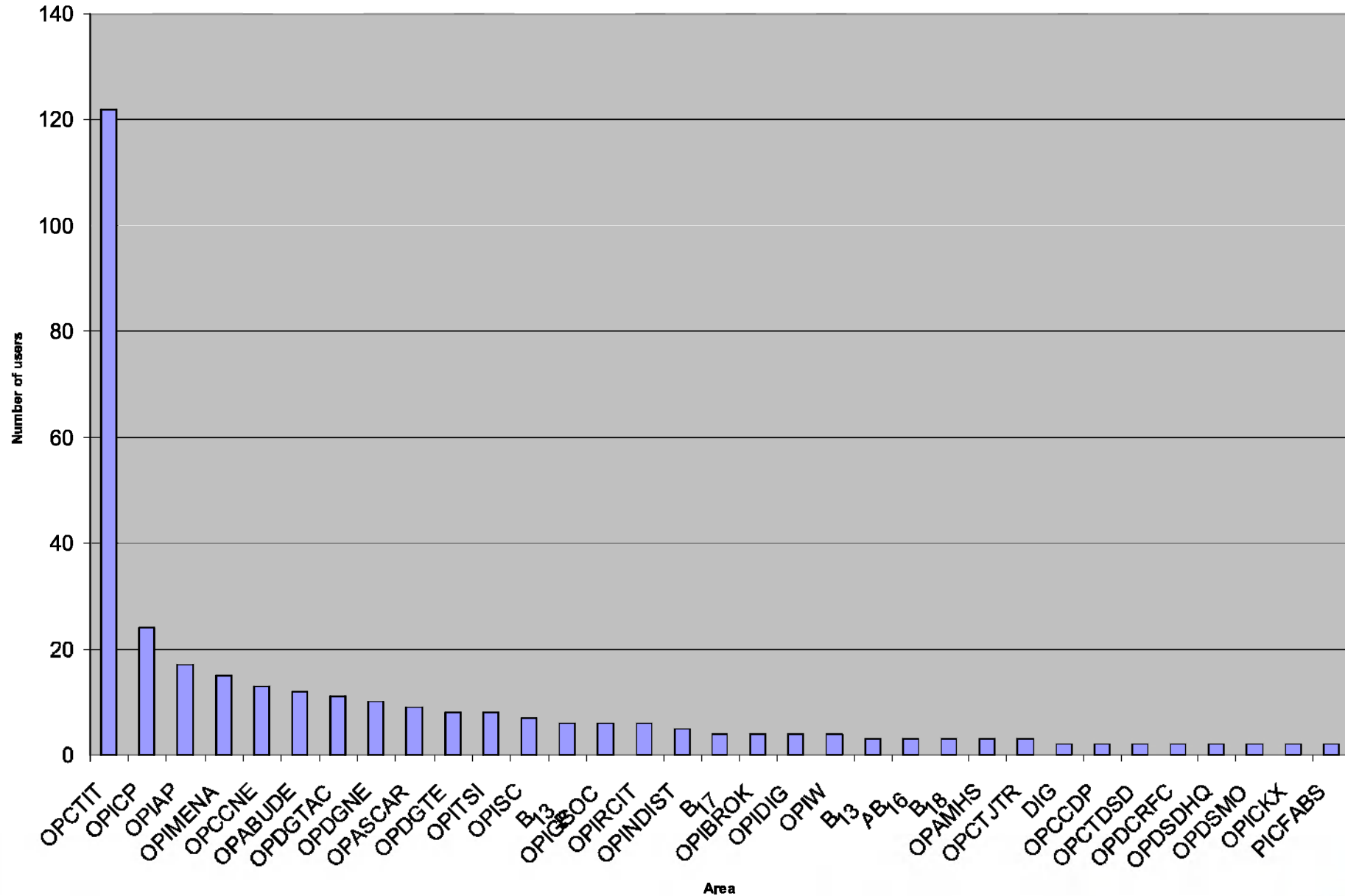
AR Prototypes - EPR Stats - Feb 2008 - Jan 2009



© Crown Copyright. All rights reserved. This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation. Refer disclosure requests to GCHQ on [redacted]. Contains Intellectual Property owned and/or managed by GCHQ. The material may be disseminated throughout the recipient organisation, but GCHQ permission must be obtained for dissemination outside the organisation.



Number of users who executed > 10 queries, by area



© Cr

other UK information legislation. Refer disclosure requests to GCHQ on [redacted]  
Contains Intellectual Property owned and/or managed by GCHQ. The material may be disseminated throughout the recipient organisation, but GCHQ permission must be obtained for dissemination outside the organisation.

