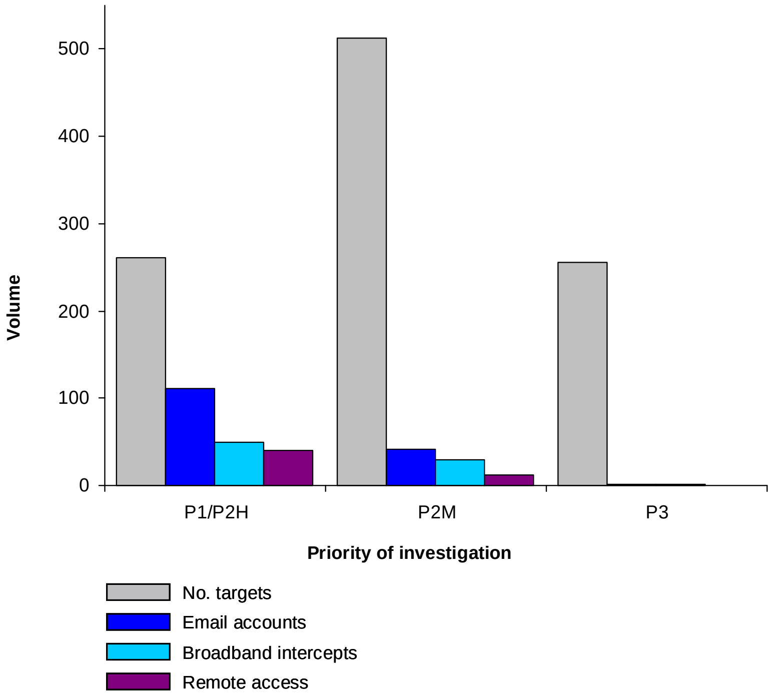
Figure 2 - Approximate coverage of targets (July 2009)



2010/11 investigative challenges

In addition to the strategic DSO coverage requirements, the investigative branches of the Service have identified a set of specific business challenges for 2010/11:

- Increasing assurance levels from 50% towards 70% for high priority investigations
- Addressing new cross border terrorist planning and commissioning threats
- Reducing the proportion of new casework with no pre-existing intelligence to below 30%
- Launching coverage of P4 targets, and providing minimum acceptable levels of coverage for non-Islamist investigations
- Addressing current workload backlogs
- Mitigating the relative lack of experience of investigative staff
- Reducing the risk of intelligence black-outs due to infrastructure failure

Capability requirements

In addition to target coverage requirements, a number of issues have been identified that demand improvements in the Service's existing DIGINT capabilities:

- There is an imbalance between collection and exploitation capabilities, resulting in a failure to make effective use of some of the intelligence collected today. With the exception of the highest priority investigations, a lack of staff and tools means that investigators are presented with raw and unfiltered DIGINT data. Frequently, this material is not fully assessed because of the significant time required to review it, particularly when pre-filtered intelligence from other sources (such as summarised transcriptions of voice interceptions) is likely to yield more value for less effort.
- The Service's processes for requesting DIGINT coverage and managing its collection are fragmented and can add administrative burden that reduces the time available for investigators to

assess intelligence. Furthermore, in some circumstances the processes do not help to maintain appropriate levels of coverage of individual targets over time.

- The capacity of the Service to maintain and develop new collection capabilities is limited: working at its maximum capacity it cannot meet all of the requests placed upon it.
- Across teams and amongst individual investigators, there is an inconsistent understanding of the capabilities currently available for the collection and exploitation of DIGINT, and there is no mechanism for sharing knowledge of evolving online behaviours that might indicate a threat or provide a disruption opportunity.
- Mechanisms for agent targeting and verification are small in scale and poorly resourced.
- The Service does not have adequate capabilities to disrupt on-line operational activities.
- The provision of business continuity and disaster recovery is inadequate for the operational systems used to receive and technically process incoming DIGINT.

To address these issues and to deliver increased assurance (in addition to significantly increasing the number of targets with DIGINT coverage), the business requirements of the Service are therefore to:

- ensure that all of the intelligence already being collected is analysed or assessed to at least an acceptable minimum level;
- exploit collected intelligence more completely and effectively, and integrate it with intelligence from other sources to derive additional value;
- develop collection mechanisms to capture intelligence that is not available from fixed and mobile broadband intercept or from the collection of customer records data, to prevent a degradation of current collection penetration;
- secure current operational IT systems (as opposed to corporate systems) by providing improved infrastructure for scalability and resilience;
- improve support for the targeting of agents and verification of agent reporting, and build new capabilities to allow disruption of on-line operational activities;
- build and maintain a workforce that understands and can keep up with the emerging threats and opportunities of the internet age.