The Digint Programme (DRAFT VERSION 0.11)

The purpose of this document to provide background for HMT and the Cabinet Office on the Security Service's Digint Programme. [Insert security/FoI disclaimer]

Defining the Digint Programme's challenge

Collecting and exploiting intelligence from the 'digital footprint' created by investigative targets presents law enforcement and intelligence agencies with new and developing challenges. These challenges increase when this material occurs in high volume for multiple targets. Some of the processes for collecting and deriving value from such material are relatively immature, others well established. There is no doubt that the take up by investigative targets of the technologies that leave a digital footprint provides a rich vein of intelligence that is set to grow in importance and cannot be ignored.

The Digint Programme is a response to four specific challenges:

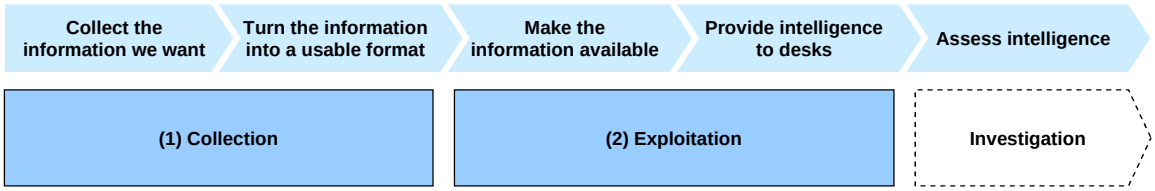
- Target use of technologies that leave a 'digital footprint' is rapidly gaining importance within intelligence investigations
- At the same time, increased usage generates a vast body of information for us to work through if we are to build a clear intelligence assessment
- The underlying technologies and behaviours create a complex and changing environment that demands a strong combination of agility and collaboration between many partners if we are to become more effective and not fall behind – and where possible increase assurance
- Improvements in this area will only represent value for money if they support capabilities that are complementary to and supportive of the two major intelligence collection programmes, IMP and SigMod

Current roles and responsibilities

HMG's response to the intelligence challenge of the Internet and Internet Protocol (IP) networks and systems is based on close cooperation and collaboration between the relevant agencies. The benefits to HMG are in the areas of enhanced national security, the protection of economic well being, and the detection and prevention of serious and organised crime. At the highest level, two disciplines must be mastered: ***(1) Collection***, which covers accessing information, capturing faithful representations

of it, and making technical sense of the 1's and 0's and ***(2) Exploitation*** which includes the processing, analysis and use of what has been collected.

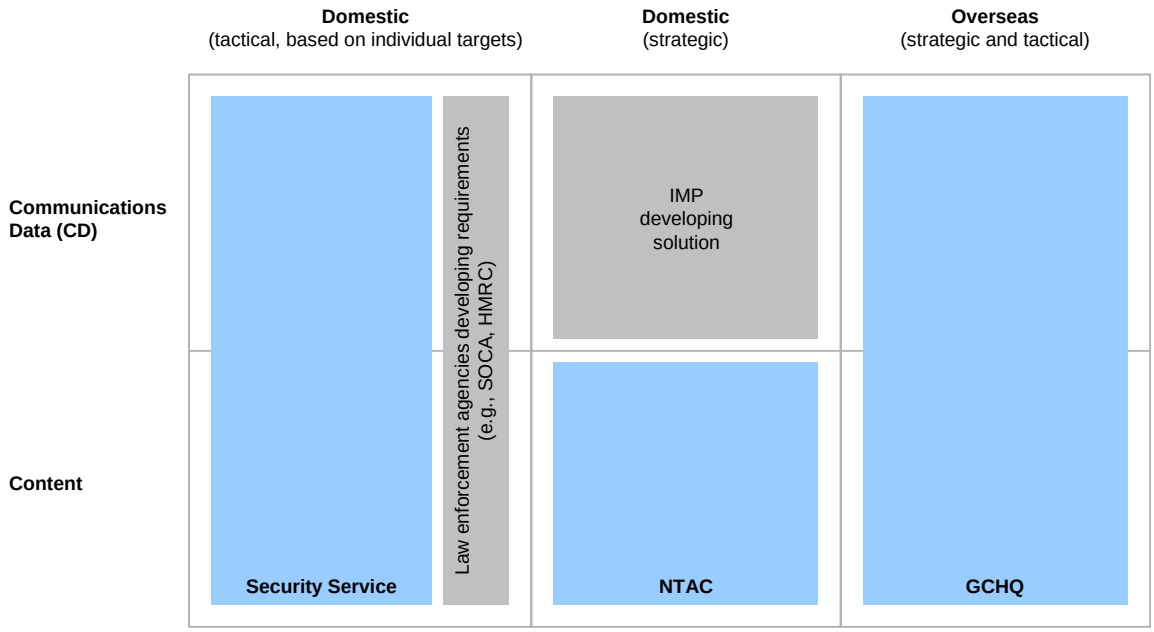
Figure 1 - Illustration of the key disciplines required to support the development of intelligence



To do this two generic types of material must be worked: ***Content*** (information generated by the investigative target, such as the words in his email) and ***Communications Data or 'CD'*** (information required by the communication service provider to allow the target to use their services, such as his subscription information via which they are able to collect payment). A further division exists between ***strategic*** collection solutions for which the technology remains in place once established, versus ***tactical*** solutions which are deployed temporarily to gather intelligence on specific high priority targets via, for example, close access and/or covert entry techniques.

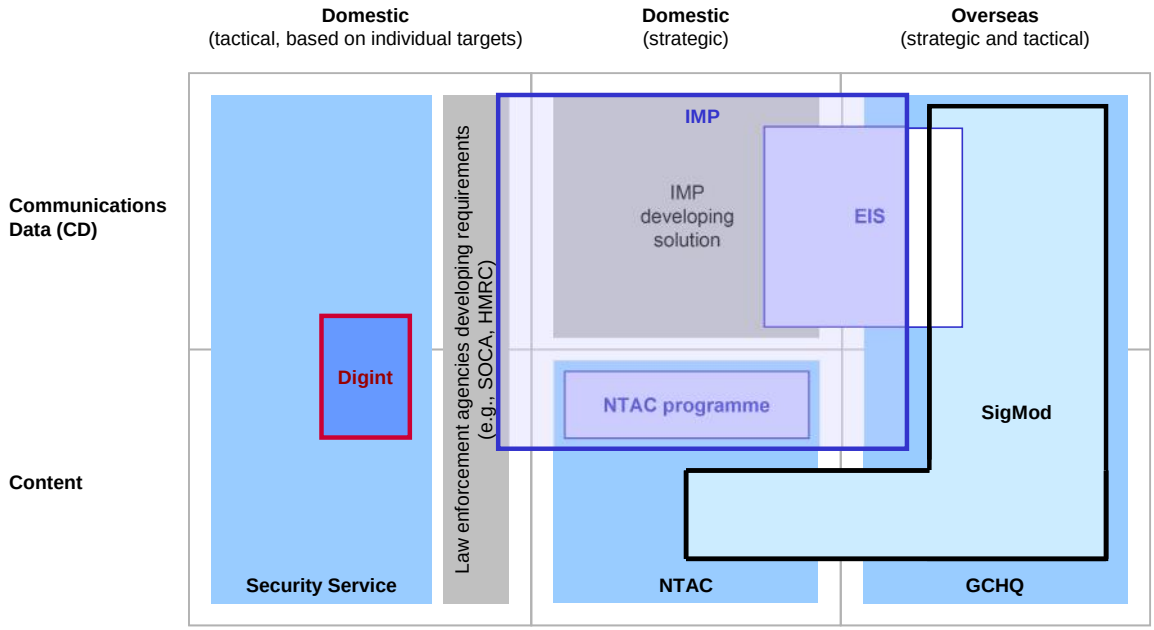
(1) Collection of intelligence from the internet, internet protocol networks and systems, and related devices

Figure 2a – Primary responsibilities



As indicated in figure 2a, the primary existing collection capabilities are cleanly allocated between the Security Service and NTAC (domestic) and GCHQ (overseas collection) with key gaps being filled by the law enforcement agencies and IMP. There are also several opportunities for collaboration and sharing of key capabilities, which become more apparent once the major programmes are overlaid, see figure 2b.

Figure 2b – Key programmes

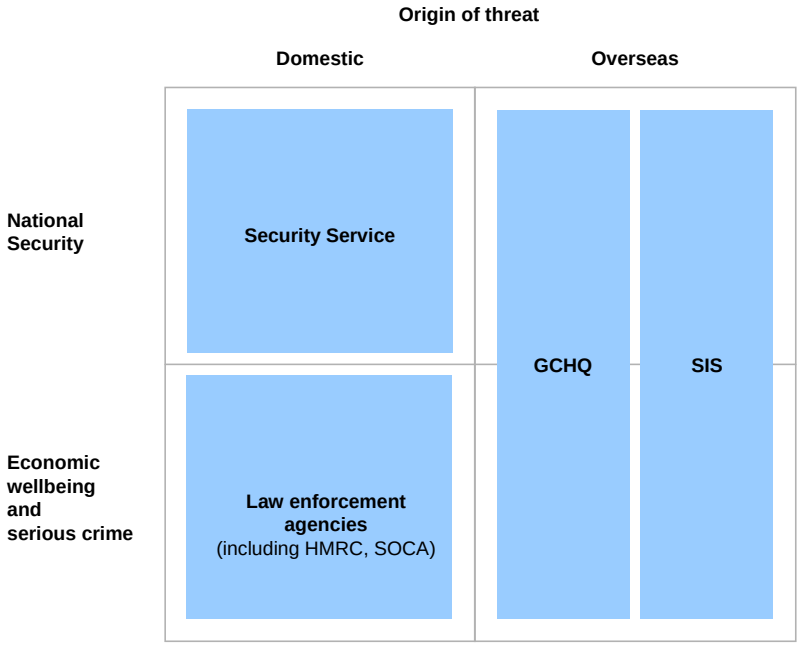


This representation also illustrates the absence of overlap between the Digint, IMP and SigMod programmes owing to the fact that each supports distinct and complementary UK collection capabilities. However, these complementarities create strong dependencies – for example, the Digint Programme could continue to deliver benefits in isolation of IMP, but would fail markedly to achieve its overall assurance objectives were it not for the NTAC and EIS capabilities that IMP is driving.

(2) Exploitation of collected intelligence

Exploitation responsibilities are allocated along similar geographic lines, as shown in Figure 3.

Figure 3 – Key exploitation responsibilities



Close partnership is essential to effective exploitation because, due to the nature of modern communications networks, the line between 'domestic' and 'international' is often blurred. In particular, domestic terrorists will often receive recruitment, radicalisation, fundraising, propaganda, or even direct command and control from overseas. Even as early as 2003, Operation OVERT found evidence of each of the above internet uses.

Further details on the roles and responsibilities associated with the above images are contained in the annex to this document.

The Security Service's response

In the area of national security the Security Service is already finding that its investigative targets use the internet, computers and smart phones extensively – including the advanced capabilities they offer. This is particularly the case in its CT work. Because terrorist planning can often span many countries, the internet provides an important tool to terrorists for communication with contacts overseas. It also offers to them apparent security benefits (although these are often perceived rather than real). As a result, collecting and exploiting this sort of target usage of technology offers real value to counter-terrorism both within the UK and outside. This includes 'upstream work' where investigations focus on threats posed to the UK by individuals based in foreign countries.

The Digint Programme

The Security Service's **Digint Programme** is being set up, with support from GCHQ, SIS, and the IMP Programme to transform its ability to work with Internet and other IP data, specifically for CT, but more generally for wider national security purposes. At this stage, the programme has three main ambitions:

1. **Build the foundations of a strategic capability with our partners**

   The Digint Programme, NTAC, GCHQ and the IMP are dependent on each other to address collectively the challenges of 'the internet age' and its associated threats to national security. We have to work together if we are to solve this difficult problem and provide the desired level of assurance.

   This joint approach will also contribute value for money by avoiding duplication of spend, sharing relevant tools and tradecraft, and focussing investment on those parts of the intelligence apparatus best placed to deliver. In particular:

   - GCHQ's SigMod transformation and GCHQ and IMP's EIS capability will substantially enhance the breadth and depth of intelligence collected and exploited from overseas upon which the Service will be able to draw, thereby reducing the volume of collection for which it would need to find a tactical collection solution.
   - GCHQ and IMP's NTAC Programme will deliver a strategic domestic content collection capability that will also begin to reduce the requirement on the Service to deliver new tactical collection activities.
   - The Service's Digint Programme focuses investment on the narrow range of tactical collection activities that offer greatest assurance with respect to the activities of key investigative targets, and on those exploitation activities that will drive greatest investigative benefits with respect to UK domestic threats.

   In turn, the data, tools and intelligence that results from these activities have been shown to enhance the efficacy of the key strategic solutions already mentioned, and will continue to do so.

2. **Solve the immediate challenge**

   The Security Service has already become the principal collector and exploiter of targets' digital footprint in the domestic space. By dint of its specific needs and role, some of the techniques it uses are unique to the Service. But its

efforts, which have already grown significantly over the last few years are in imbalance. It can currently collect (whether itself or through partners such as NTAC) significantly more than it is able to exploit fully. This creates a real risk of 'intelligence failure' ie from the Service being unable to access potentially life-saving intelligence from data that it has already collected.

The Service's primary need therefore is to develop at pace through the Digint Programme capabilities (i.e. processes, people and technology) which will enable it to improve investigative value from its collection investment, now and in the future, in a way that is compatible with developments in IMP and GCHQ.

3. Extend coverage

Given the increasing importance of a target's 'digital footprint' to investigations, a substantial increase in coverage is required. The Service therefore seeks to collect and exploit more material, and its target is double what it currently collects by end FY 10/11 so as to allow coverage of all priorities of CT investigation.

The enhanced capabilities will be targeted and specific in scope and thus will satisfy the central legal requirements of necessity and proportionality, as well as being cost effective. They are also well placed to address growing evidence of threats coming from people on the peripheries of investigations, the events on Christmas Day in Detroit being a recent example.

Successful achievement of ambitions 1 and 2 will be essential if we are to protect our existing capabilities in the face of evolving technology and target behaviours. Ambition 3 will need to adapt to any shift in the level of terrorist activity or the level of assurance that the Service is required to provide.

Further details around the programme's approach and benefits can be found in the 6th November 2010 Digint Strategy and the Digint Programme's draft Outline Business Case. This latter document is seeking HMT approval during March 2010.

Annex – further description of current roles and responsibilities

- *Collection* responsibilities may be further divided into five broad categories, based principally on geography (Domestically or Internationally -focused) and scale (Strategic or Tactical):

    - **Strategic (large-scale, enduring) domestically-focused collection of Content** day to day is the responsibility of NTAC, which is accountable to Director GCHQ. The Interception Modernisation Programme (IMP)[1] is responsible for funding NTAC's transformation of its domestic Content collection operations so as to be fit for purpose for the internet and IP networks.

    - The IMP is also responsible for providing the future IP **Strategic domestically-focused collection solution for CD**. At present, the Communications Service Providers provide requested CD direct to the agencies that need it. Determining an 'internet-proof' solution for CD – i.e. one that can address the growing range of services available to internet users while maintaining HMG capabilities to provide CD that can be used in evidence by Law Enforcement agencies – requires legislative change which IMP must deliver.

    - Individual agencies develop and deploy methods for **Tactical (small-scale, short-term) domestically-focused collection of Content and CD** where the strategic solutions are inadequate. To date this has mainly been by the Security Service, although others such as SOCA and HMRC are developing requirements in this space.

    - **Strategic internationally-focused collection of Content and CD** falls to GCHQ. Its 'Mastering the Internet', 'Better Analysis' and 'Support to Military Operations' programmes address the requirements in this space.

    - **Tactical internationally-focused collection of Content and CD** is also worked by GCHQ, filling gaps on a case by case basis often in partnership with SIS and MoD.

[1] Managed by the Home Office's new Communications Capabilities Directorate

- *Exploitation* responsibilities are divided primarily by geography and purpose. For example, is there an overseas threat to our national security, is there a domestic threat to the nation's security, or are we working to secure an important criminal conviction?

    - the Security Service leads for national security purposes on exploitation of the digital 'footprint' created within the UK by investigative targets. It does this in close partnership with GCHQ which concentrates principally though not exclusively in the exploitation of targets overseas. SIS helps fill some niche gaps outside the UK. Close partnership is essential because, due to the nature of modern communications networks, the line between 'domestic' and 'international' is often blurred. In particular, domestic terrorists will often receive recruitment, radicalisation, fundraising, propaganda, or even direct command and control from overseas. Even as early as 2003, Operation OVERT found evidence of each of the above internet uses.

    - GCHQ (often in partnership with SIS and with occasional niche assistance from the Security Service) leads on exploiting communications and IT networks for the purpose of countering national security, economic well-being and serious crime threats that originate from overseas.

    - Law enforcement agencies (including SOCA and HMRC) exploit communications in support of the detection and prevention of serious and organised crime. They are assisted in this by GCHQ and, on occasions, SIS for targets overseas and by NTAC for targets in the UK.