UK Government Organisations Involved in Communications and Information Systems Security

by Dr Brian Gladman, Worcester, June 1999

Introduction

This summary of UK government ‘information security’ organisations was first published on the ‘uk-crypto’ mailing list. This version is mostly a copy of the original posting but there is a small amount of new material. I would like to acknowledge the contributions made by Peter Somner, Duncan Campbell and other list members in providing additional aspects included in this version.

The Government Communications Headquarters (GCHQ)

GCHQ is the UK's electronic intelligence collection agency - the jargon term for this is SIGINT - short for Signals Intelligence. It has its Headquarters in Cheltenham and its collection facilities are located at many sites both in the UK and overseas. It undertakes collection, decryption, language translation and, for some traffic, interpretation as well. For other types of traffic it acts as a primary collection and code-breaking agency but passes the resulting information to expert cells in other government departments for interpretation (for example, the Defence Intelligence Staffs in MOD).

It has enormous collection resources, shared with NSA, and a wide range of general purpose and custom designed computer systems for code breaking. Recently its activities have received considerable exposure with the publication of Duncan Campbell’s report on Echelon for the European Parliament.

GCHQ is a part of the Foreign and Commonwealth Office and some details of its functions and the statutory basis for them are set out on its web site. Historically its role has been the collection of intelligence information but its statutory duties (set out on its web site) include:

- to monitor or interfere with electromagnetic, acoustic and other emissions and any equipment producing such emissions and to obtain and provide information derived from or related to such emissions or equipment and from encrypted material

This shows that it is allowed to interfere and disrupt communications systems and services if it chooses to do so.

There are some within government who believe that the above description gives GCHQ a mandate to penetrate computer systems both for information collection and for active disruption and deception attacks. However others dispute this and believe that there are immense legal problems in this area of operation. So far these uncertainties appear to have limited the extent to which GCHQ has deployed operational capabilities in this area (cal led Offensive Information Warfare)

The Communications Electronic Security Group (CESG)

CESG is the part of GCHQ that is responsible for protecting UK government communications. In the jargon this is COMSEC - communications security. It also has responsibility for computer security - COMPUSEC - and for protective information security - INFOSEC. It likes to be called the 'UK National Authority' for such matters although its mandate in respect of other government departments is formally only advisory.

Its main responsibility is for designing and approving cryptographic algorithms for UK government use and for implementing them in prototype form. For some government departments it also builds complete systems but for others it simply supplies cryptographic algorithms or hardware. It is located on the GCHQ Benhall site in Cheltenham.

CESG has responsibilities in information security and is involved in computer systems security and in the design of secure networks and protocols. However, historically its main activity has been in the design and construction of cryptographic hardware and this has meant that it lacks the culture needed to be effective in the computer systems field. Moreover it has never had sufficient staff or financial resources to tackle this area of R&D effectively. This has led to R&D failures and policy advice to other government departments that has been unrealistic. This has had a damaging impact on the performance, cost and affordability of their operational computer systems. MOD has suffered especially badly here.

CESG used to be funded centrally but they have now moved onto a repayment basis in which a significant part of their income has to be obtained from their customers for the services they provide. This should in time bring about a change in culture and may overcome the difficulties that they have had in developing effective policies in the computer systems area.

However CESG remains a part of GCHQ and this means that its primary objective in respect of any cryptography outside of its direct control is to ensure that it is ineffective. This means that the CESG interest in respect of preventing information warfare attacks on the UK, government assets aside, is hence highly suspect.

CESG represents UK government interests on a number of international committees that deal with either communications or information systems security. CESG staff have a role alongside DTI in the European Union 'Senior Officials Group on Information Security' group. Here they have a reputation for ensuring that no serious research and development is sponsored in European Commission R&D efforts.

In the UK, CESG are sponsoring the development of Public Key Infrastructure (PKI) developments for use within government departments. It also appears that they are promoting these or related activities as a basis for information protection in the National Health Service and in the provision of government services to the public using electronic networks. This work has been criticised by Dr Ross Anderson and others both in terms of technical weaknesses and in respect of its poor match to the true needs of intended user communities.

There may be a battle ahead since the deployment of these technologies to protect the UK public will open up the question of the true role of CESG. Historically CESG has prevented any effective protection of information outside of government in the UK in order to protect the intelligence collection capabilities of its parent organisation, GCHQ. But, protection of National Health Service information and other information owned by UK citizens conflicts with this historic approach and requires true protection for non-government data.

So far CESG have sought to promote 'key escrow' solutions but these do not seem likely to survive since the UK businesses and private citizens are very hostile to their use. At the moment, therefore, CESG still seem to be following their traditional policy but this might now be changing slowly.

The Ministry of Defence (MOD)

A major MOD responsibility is that of collecting and analysing military intelligence data. The staffs involved are highly professional and very careful to ensure that their work does not stray over the boundary into activities not soundly based within the statutory responsibilities of the MOD. I am obviously biased but I consider them a national asset and not a threat to the privacy of UK citizens. MOD has its own collection assets buts also relies heavily on GCHQ.

The MOD is a major customer for GCHQ intelligence data and a major user of secure communications and information systems. As such it is a major client of both GCHQ and CESG. In respect of cryptographic products MOD has been CESG's major customer and has in the past taken as much as 90% of their output.

MOD relies on CESG for the design of cryptographic algorithms and prototype designs but does most of its own development and production work through its Procurement Executive in Bristol. Except for cryptographic algorithms MOD has an independent mandate to undertake its own programme of research and development in respect of communications and information systems security.

In principle MOD does not have to apply CESG rules, or take their advice, but in practice it almost always does, even when it is aware that it is flawed. This is engineered through a careful 'conspiracy' between CESG and GCHQ: if MOD does not accept what CESG tells them to do GCHQ then threatens to cut off MOD's intelligence data feed on the pretext that MOD computer systems are not secure enough to handle it.

The only area of MOD to avoid this 'blackmail' is the MOD Procurement Executive in Bristol, which, because it does not need much GCHQ intelligence, has been able to implement reasonably effective and secure computer systems to support its operations.

MOD staff at all levels are well aware that GCHQ advice (and that is what CESG advice is) is wasting large sums of taxpayers money but they don't do anything about it for fear of upsetting GCHQ.

The Defence Evaluation and Research Agency (DERA)

DERA is the research arm of the MOD, now running as a semi-autonomous agency reporting direct to the Minister of Defence. It has a large number of sites in the UK (and some overseas) but information security work is largely concentrated at Malvern in Worcestershire. It is tasked by the MOD to conduct research into information security issues and undertakes work in both offensive and defensive techniques. Until the mid-1980s it was the only government organisation with a significant information security research programme and its work on computer and network security predates that at GCHQ by at least 10 years.

DERA at Malvern (then the Royal Radar Establishment and the Royal Signals and Radar Establishment) was an early participant in ARPANET and a leader of UK research and development in the defence packet switching field. In the 1980s it sought to design and develop secure computer systems for defence use but none of these achieved any significant success. It was somewhat more successful in designing packet switching encryption products and these eventually went into MOD service.

In the mid 1980s GCHQ sought to take over and remove the DERA mandate for research in the computer and information security fields. It seems likely that this was a move designed to ensure that GCHQ maintained control of government R&D in this field. The DERA success in designing a packet switching encryption product before the US almost certainly prompted NSA to encourage GCHQ to make this move in order to retain control over the technology.

After a considerable period of infighting GCHQ succeeded in getting CESG nominated as the 'UK National Authority' for information security but DERA secured an agreement in which they retained a the right to conduct independent R&D in the computer and information security fields.

DERA has undertaken work under contract for GCHQ and CESG in the computer, network and software security fields.

In my (biased) view DERA remains the most competent organisation within government in the secure computing and networking fields. However it appears to be losing this expertise as declining budgets and increasing “chief/Indian ratios” cut into its research programmes.

The Department of Trade and Industry (DTI)

The DTI's role in cryptography and information security is to manage the industrial and economic aspects of the topic and to co-ordinate the 'public facing' aspects of cryptography and information security policy such as, for example, export licensing. They therefore have the unenviable task of bringing UK government departments together in order to set a coherent UK government policy on cryptography and information security matters.

They represent the UK on the EU bodies dealing with these subjects and also attend activities such as the Wassenaar Arrangement where cryptography controls are agreed.

They used to rely on the National Physical Laboratory and on DERA Malvern for technical expertise but shifted to employing commercial resources in the 1980s. They now have no significant intramural technical expertise in the field (although some of their staff are individually competent).

The DTI also lead in a number of activities designed to exert control over the form in which cryptography is used in telecommunications systems. As an example, a senior DTI official leads the committee work within the European Telecommunications Standards Institute (ETSI) to ensure that any deployed cryptography is weak enough to allow the security and privacy of end users to be compromised without their consent. This work is an example of DTI ‘looking both ways’, that is, wanting to appear ‘electronic commerce’ friendly in public while doing the dirty work of GCHQ and Home Office behind the scenes.

But there are now some signs that DTI is moving away from this position and may in future leave other departments to do their own dirty work so that DTI can increasingly become a true champion of electronic commerce (and, maybe, even the privacy rights of UK citizens!). Watch this space.

The Cabinet Office

The Cabinet Office manages the central intelligence machinery and runs a number of committees that have a role in considering cryptography and information security issues. It has a major role in deciding departmental responsibilities where new issues arise or where the departments are unable to agree on how things should be handled. The departmental responsibility for protecting the UK in the face of electronic attack on our information infrastructure is a hot topic at the moment. There is some evidence to suggest that they see the term 'electronic attack' as covering much less than 'information warfare' and, if true, this leaves the issue of the responsibility of protecting the UK in the face of an information warfare attack unresolved.

The Cabinet Office is also responsible for the Central Information Technology Unit (CITU)

Central Information Technology Unit (CITU)

CITU is responsible for Information Technology policy and strategy spanning government departments and for the promoting the use of IT in the delivery of government services to the public. They are taking the security and privacy aspects of their tasks seriously.

GCHQ have been trying very hard to interest CITU in their insecurity products but senior CITU staff is very well aware that public trust and GCHQ involvement are likely to be mutually exclusive. CITU are relying heavily on industry involvement to obtain an effective strategy for secure service delivery but the extent to which their proposals have been subject to scrutiny by independent experts is unknown to the author.

The Central Computer and Telecommunications Agency (CCTA)

The CCTA also handles pan-government matters in Information Technology and Telecommunications and provides resources to support those government departments that do not employ their own expert IT staff.

Until the early 1990s the CCTA had responsibility for setting policy on the security and privacy protection required for all government information designated as 'sensitive but unclassified'. In outline classified information is information which, if revealed, would damage the UK – this was handled by CESG with CCTA handled the rest. However when they became interested in cryptographic protection in the early 1990s, CESG moved immediately to take over their duties in setting protection policy for this class of information (see the trend here!). Although a number of staff in CCTA were acutely aware of the damage this would do, CCTA was no match for the political power of GCHQ and these responsibilities were eventually transferred.

So GCHQ insecurity policies now apply on a pan-government basis!

The Security Services

The Security Services are responsible for assessing the threat to the UK in respect of information warfare (and some other) forms of attack. As a part of this they have taken over the sponsorship of CRAMM, an approach to risk analysis.

They are also responsible for approving individuals and companies to handle government classified information.