Software Reverse Engineering
Network Defence performs reverse engineering both of malicious and of non-malicious code – i.e,.code is translated from machine-readable to human-readable form so that its functions and vulnerabilities can be analysed more easily. Analysis of non-malicious code is undertaken for two main reasons – to establish the vulnerability of Operating Systems and applications to electronic attack, and to authenticate the claims made for security-related products and their general suitability for HMG use. All this knowledge informs CESG's advice to HMG on electronic attack.

Network Defence's SRE work is mainly in support of the Response and IA teams, but occasionally for other parts of GCHQ and external customers. Within ND, both the VR and the ID teams perform SRE work.

PoCs: [redacted] (VR), [redacted] (ID).

Main Customers
Internal (CESG/GCHQ), HMG.

Sources: where does the material come from?
Malicious code is acquired via various routes – HARUSPEX/GORDIAN KNOT, OGDs, commercial organisations.
Non-malicious code is acquired through normal commercial channels.

"Target" location
Not applicable

Legal Authorities
Reverse engineering of malicious code does not require a warrant, because there is no agreement with the author that would be breached by carrying out that activity.

However, reverse engineering of commercial products needs to be warranted in order to be lawful. Network Defence may rely on GCHQ's SRE warrant (GPW/1160, renewable every 6 months). There are some limitations to this warrant – it only covers us under UK law, for example, and it only authorises work conducted for a SIGINT or IA purpose. The authorisation for ND's SRE work has been discussed with [redacted], the SRE co-ordinator for CCNE.

Local authorisation forms for commercial SRE work under this warrant are signed by [redacted] (for the ID team) or by one of a list of named individuals (for the VR team). Because it is hard for the ID team to predict which products it may have to reverse engineer, and such work may need to be authorised at short notice, ID team SRE work is authorised en masse on a yearly basis. *Who approved this arrangement?*

Input from VR/ID is required every 6 months to support GCHQ's SRE warrant renewal. This can be based on the local authorisation forms for that period.

***Note**: Until Feb 08 the ID team were not following the internal authorisation procedure. This error was reported on 29/0/08 and has now been corrected. SRE performed by the ID team before that date has been authorised retrospectively.*

Local Policy statements
The Internal process for authorising SRE work is described at:
http://www.[redacted]/sreleg.shtml

GCHQ's latest SRE Warrant:

9014a GPW1160
SRE renewal Jun0…

See also [redacted]'s emails of 14/1/08, 23/6/08.

Details of team SRE work, including completed authorisation forms and the list of people who can authorise VR team SRE work:
T:_I\IA RA 1\CESG_Network_Defence\XTNS\XTNS Staff Only\VR\SRE
T:_I\IA RA 1\CESG_Network_Defence\Documentation\3.5 ID Malicious Code Research_SRE Legalities

Auditing arrangements
The following are responsible for ensuring that ND's SRE work complies with the terms of the warrant, if applicable:
List of local authorisers (VR team)
[redacted] (ID team)

Status:
Updated 15/7/08, following meeting with [redacted]