[Exhibit 4]

The underlined parts of this document indicate that it has been gisted for OPEN

Extract from current Advanced Training for Active Operations

CNE involves gaining remote access to computers and networks and possibly modifying their software without the knowledge or consent of the owners and users with the aim of obtaining intelligence.[1]

CNE operations must be authorised under ISA s.5 or s.7, depending whether the target computer or network is located within or outside the British Islands.

If you're working under a s.7 authorisation and find that the target computer has been brought to the UK, you should inform the relevant team immediately.

ISA permits a period of 5 working days before the presence of the implanted computer in the UK makes our action unlawful. You will have to fill out a form to register that you are in the "5-day grace period" and you may need to seek a s.5 warrant before the period expires.

No specific authorisation is required for developing CNE implants and techniques (no unauthorised access occurs), but testing may require authorisation. [2]

CNE operations carry political risk. These risks are assessed by the relevant team – consult them at an early stage if you're considering a CNE operation.

---

[1] Underlining in original.
[2] Both instances of underlining in this paragraph are in the original.