small arms, mortars, bombs and mines. Definitions of terrorist threat levels are at Annex D. See also Chapter 7.

Non Traditional Threats Posed by Other Individuals or Organizations

0111. Government assets are under threat from a variety of sources beyond those traditionally regarded as hostile or otherwise of significance in terms of national security. The responsibility for providing advice to counter non-traditional threats will not always lie with the security staff and may often be provided by the appropriate Service, MOD or civil police agency. The main threats of this type are posed by investigative journalists, pressure groups, investigation agencies, criminal elements, disaffected staff, dishonest staff and computer hackers. The types of threat from these sources can be categorized in six broad groups:

a. **Confidentiality**. Compromise of politically sensitive information. This threat is presented by:

(1) Pressure groups and investigative journalists attempting to obtain sensitive information.

(2) Unauthorized disclosure of official information (leaks).

b. **Exploitation of Sensitive Information.** Debt collection agencies and investigation agencies are known to attempt to obtain personal information held in confidence by government. Investigative journalists have exploited personal tax information; they also target commercial and financial information as do criminal elements seeking financial advantage.

c. **Theft, Burglary and Fraud.** There is a growing threat of theft, particularly of IT equipment. Arms, ammunition and explosives are always at particular risk. Theft may occur through burglary or the actions of dishonest staff. Establishments responsible for the collection or disbursement of public funds are prone to fraud and there is an increasing threat of fraud through the manipulation of IT systems.

d. **Corruption, Destruction, or Unauthorized Access to, Computer Data.** The integrity of data held on computer systems is under threat mainly from disaffected staff. Existing levels of programming expertise, the ready availability of malicious software, e.g. viruses, and the ease with which they can be deliberately or accidentally introduced, combine to create a substantial threat. It is apparent that some staff misguidedly interfere with or compromise systems. There is also a level of threat of damage resulting from the actions of hackers - either those with legitimate access to systems or those without such access.

e. **Pressure Groups.** Pressure groups for such causes as animal rights, nuclear disarmament and the environment will sometimes carry out demonstrations against MOD policy and activities. Although often confined to peaceful demonstrations, extremist elements can cause violent attacks on individuals and property, which can pose a threat as significant as terrorism.

f. **Criminal Damage.** Employees, dependants, visitors or intruders can carry out criminal damage.

g. **Natural Disaster.** Natural disasters are risks to the integrity or availability of facilities, buildings or equipment etc caused by such incidents as fire, flooding, subsidence, or lightning strike.

Components of Security

0112. There are two different and interdependent parts of security:

a. **Security Intelligence.** The collection of information and production of intelligence concerning the security threat. Plans to counter the activities of foreign intelligence services or subversive organizations and individuals must be based on accurate and timely intelligence concerning the identity, capabilities and intentions of the hostile elements. This intelligence is known as 'security intelligence'. It is derived from studying attempts to break through security controls, combined with knowledge gained from penetrating hostile organizations. One means of obtaining security intelligence is the investigation of breaches of security. Although security intelligence is a matter which is principally the concern of security staffs and security units, all personnel in the MOD, whether Service or civilian, contribute to it by the prompt reporting of suspicious activity.

b. **Protective Security** - consists of:

(1) **Laws, Orders and Instructions**. These measures range from the Official Secrets Acts to Establishment Security Standing Orders.

(2) **Physical Measures**. Physical measures are the physical obstacles, which protect specific security interests. These range from perimeter defences such as fences and lighting to security containers.