and controlled by computers. In the past a common a failure in the computer system that controls the network and attacks on networks were mainly directed towards these computers. Nowadays, the most disrupting attacks tend to exploit the weaknesses and vulnerabilities of network components (operating systems, routers, switches, name servers, etc.).

Whilst disruptive attacks on the telephone system have not been a major concern in the past, attacks on the Internet are quite common. This is due to the fact that telephone control signals are separated from traffic and can be protected whereas the Internet allows users to reach the key management computers. However, the telephone network may become more vulnerable in future as it will integrate key elements of the Internet and its control plan will be opened to others. Attacks may take various forms:

Name server attacks: The Internet depends on the operation of the Domain Name System (DNS) through which user-friendly names are translated into abstract network addresses and vice versa. If part of the DNS fails, some web sites cannot be located and email delivery systems may stop working. Corruption at the level of DNS root servers or other top level name servers could lead to widespread disruption. Earlier this year some vulnerabilities were discovered in the software on which most name servers operate.

Routing attacks: Routing in the Internet is highly decentralised. Each router periodically informs neighbouring routers about which networks it knows and how to reach them. The weakness is that this information cannot be verified because, by design, each routerôs knowledge of network topology is minimal. In consequence, any router can represent itself as a best path to any destination as a way of intercepting, blocking or modifying traffic to that destination.

Flooding and denial of service attacks: These forms of attack disrupt the network by overloading it with artificial messages which deny or reduce legitimate access. It is similar to fax machines being blocked by long and repeated messages. Flooding attacks attempt to overload web servers or the handling capacity of Internet Service Providers (ISPs) with automatically generated messages.

Potential damage - Interruptions have been damaging for certain high-profile websites. Some studies have calculated several hundreds of millions of Euro of damage from a recent attack, in addition to the intangible damage to reputation. Increasingly companies rely on the availability of their websites for their business and those companies that depend on it for ójust in timeô supply are particularly vulnerable.

Potential solutions - Attacks on DNS servers are, in principle, easily dealt with by extending the DNS protocols, for example using secure DNS extensions based on public key cryptography. However, this involves installing new software on client machines and has not been widely deployed. Also, the administrative process required to enhance the trust between DNS domains needs to become more effective.

Attacks on the routing system are much harder to defend. The Internet was designed to maximise flexibility in routing as this reduces the probability of service being lost if one part of the network infrastructure breaks down. No effective means exist to secure routing protocols, especially on backbone routers.

The volume of data transmitted does not allow for detailed filtering as such verification would bring the networks to a halt. For that reason only basic filtering and access control functions are performed by the networks, whereas more specific security functions (e.g. authentication, integrity, encryption) are placed at the boundaries of the networks i.e. on the terminals and network servers that act as end points.