

EU tables cyber-crime proposal

By Michelle Price

Information Age, May 23, 2007

http://www.information-age.com/infolog/ia_today/2007/05/eu_tables_cybercrime_proposal.html

The European Commission has tabled a proposal on how to tackle issues surrounding high-tech crimes, including online fraud, pornography and hacking, in recognition of the increasingly widespread and sophisticated nature of cyber threats, it was revealed on Tuesday.

The EU home affairs commissioner Franco Frattini, who proposed the paper, said that there “is an urgent need to take action at national, European as well as international level,” and added that public-private cooperation, in particular information sharing, would be critical. Brussels will be launching an initiative to encourage information exchange between police, judicial and administrative authorities and the business sector, as a result.

The business community and ISPs are generally reluctant to disclose incidents of cyber-crime or information theft, for fear of reputational damage. “However, such information may be needed if public authorities are to formulate an efficient and appropriate anti-crime policy,” Frattini writes in his paper.

Commenting on the recent EU proposal, Dr Andrew Colarik, an expert on cyber-warfare and co-author of the recently published *Cyber Warfare and Cyber Terrorism* told Information Age: “Every nation that relies on information technology for its economic sustainability and growth must address the security of [its] infrastructure.” However, he adds, the “critical component to securing our economic infrastructures requires true leadership.”

The profile of cyber-crime, cyber-terror and cyber-warfare was thrown into the public spotlight this month, with the unprecedented wave of cyber-attacks perpetrated against Estonian electronic infrastructures following an inter-regional dispute with neighbouring Russia. In April, Information Age reported on the increasing scope and risk of the cyber-assault threat, in which a range of tactics, including hacking and denial of service, are deployed to disrupt, corrupt or steal data from target computer systems.