Cybercrime. The Dark Side of Technology:
Some Reflections on the interdisciplinary issues

Frank Land

London School of Economics

In this talk I want to explore some topics that were receiving a great deal of attention from the media and in particular the computer press as well amongst IS practitioners, management and academia. The topic was the apparently rapidly growing threat coming from the misuse or criminal use of information and communications technology (ICT) as well as the use of the technology in warfare (Cyberwarfare). The issues were discussed under a variety of labels but usually included terms such as security, privacy, risk and evasion of intellectual property regulations or piracy.

However, though these topics were receiving a great deal of attention and indeed academic research, most attention was paid to ways of defending users and systems against the threats looking at the issues as primarily technical matters of technical concern needing technical solutions.. There was little recognition that the problems could only be understood in the context of interdisciplinary studies.

The talk draws attention to two issues:

The first is of the opportunity provided by the omniscience of ICT for people and organisations to engage in a large variety of anti-social or dubious practices as well as practices which defy authority in what many regard as the public interest of which Wikileaks is one example. Technology is neutral in value terms and that entrepreneurs and innovators using the technology do not all share the values which seek to use technology to enhance the lot of mankind.

The second is how the use of ICT, often regarded as the mainspring of what has been labeled the *'knowledge society'* has nevertheless led to a *'knowledge paradox'*, with counter-knowledge (Thompson, 2008) rivaling 'true' knowledge in its prevalence.

Thompson, D., (2008), *Counterknowledge: How We Surrendered to Conspiracy Theories, Quack Medicine, Bogus Science and Fake History*, Atlantic Books, London