The “Inverse CSI Effect” in Digital Forensics

Richard E Overill

Department of Informatics, King’s College London, Strand, London WC2R 2LS

richard.overill@kcl.ac.uk

Abstract

The “CSI Effect” has been well documented in recent years. In essence, as a result of viewing the several “Crime Scene Investigation” TV series, jury members and legal personnel not possessing technical competence have come to expect unambiguous results of forensic tests to be provided by forensic scientists virtually instantaneously and in all circumstances. These unrealistic expectations, fuelled by the need for dramatic licence on TV, have inevitably resulted in disappointment and incomprehension when confronted by the contingent, probabilistic and often time-consuming nature of actual forensic tests.

In this paper we introduce the “Inverse CSI Effect” which considers how an actual or potential criminal might be expected to react to the CSI Effect in terms of modifying their modus operandi (MO). In particular, we examine how the Inverse CSI Effect might be expected to operate within the digital forensics paradigm. This leads on naturally to some predictions regarding future trends in the behavioural profiles of cyber-criminals.

If the CSI Effect causes many cyber-criminals to believe that unambiguous digital evidence of their activities can be routinely obtained almost instantaneously, they are likely to modify their MO in a number of ways. They are likely to withdraw from cyber-criminal activity that now appears too risky in the light of the perceived ease of discovery. They may migrate to alternative modalities involving many layers of concealment, stealth and obfuscation. The up-front investment required to implement these advanced methodologies will necessitate a proportionate increase in the expected returns, in order to maintain a stable cost-benefit ratio. Thus we would anticipate a compensating increase in the average value of cyber-crime heists, accompanied by a migration to sophisticated strategies of concealment.