MISSED SOLUTIONS TO WWII ENIGMA DESIGN WEAKNESSES

Harold Thimbleby

Swansea University, Wales UK

The German World War II Enigma suffered from design weaknesses that facilitated its large-scale decryption by the British throughout the war. The main technical weaknesses (self-coding and reciprocal coding) could have been avoided using simple contemporary technology, and therefore the true cause of the weaknesses is not technological but must be sought elsewhere: we argue that human factors issues resulted in the persistent failure to seek out more effective designs. Similar limitations beset the historical literature, which misunderstands the Enigma weaknesses and therefore inhibits broader thinking about design and the critical role of human factors engineering in cryptography.

Harold Thimbleby is professor of computer science at Swansea University, Wales, and Emeritus Professor of Geometry, Gresham College, London. He built an electromechanical Enigma in 2002 to illustrate a Gresham College lecture on cryptography, and he has been fascinated by the topic ever since. Harold's research interest is human error, particularly in complex healthcare systems, but he became interested in the Enigma because its design failures (which effectively lost a war) make a provocative analogue to healthcare IT design failures.