encode messages into images, and then transported these via e-mail and possibly via *USENET* to prepare and execute the September 11, 2001 terrorist attack. The Federal Plan for Cyber Security and Information Assurance Research and Development, published in April 2006 makes the following statements:

- *<...> immediate concerns also include the use of cyberspace for covert communications, particularly by terrorists but also by foreign intelligence services; espionage against sensitive but poorly defended data in government and industry systems; subversion by insiders, including vendors and contractors; criminal activity, primarily involving fraud and theft of financial or identity information, by hackers and organized crime groups* [2, p. 9–10];
- *International interest in R&D for steganography technologies and their commercialization and application has exploded in recent years. These technologies pose a potential threat to national security. Because steganography secretly embeds additional, and nearly undetectable, information content in digital products, the potential for covert dissemination of malicious software, mobile code, or information is great.* [2, p. 41–42];
- *The threat posed by steganography has been documented in numerous intelligence reports* [2, p. 42].

Moreover, an online "terrorist training manual", the *"Technical Mujahid, a Training Manual for Jihadis"* contained a section entitled "Covert Communications and Hiding Secrets Inside Images" [1].

By early 2002, a Cranfield University MSc thesis developed the first practical implementation of an online real-time Counter Terrorist Steganography Search Engine. It was designed to detect the most likely image steganography in transit and thereby provide UK Ministry of Defence Intelligence Staff a realistic approach to "narrowing the field", suggesting that interception capacity was never the difficulty but rather prioritizing the target media.

Despite this, there are no known instances of terrorists using computer steganography. Al Qaeda's use of steganography is somewhat simpler: In 2008 a British man, Rangzieb Ahmed, was alleged to have a contact book with Al-Qaeda telephone numbers, written in invisible ink. He was convicted of terrorism [4].

Thus, steganography is a powerful tool of communication in computer networks. It also gives users a tremendous opportunity. And that is why we shall refer to steganography with caution because it can be used very effectively with evil intentions.