The advent of Deep Learning has transformed our digital society. Starting with simple recommendation techniques or image recognition applications, machine-learning systems have evolved to play games at eye level with humans, identify faces, or recognize speech at the level of human listeners. These systems are now virtually ubiquitous, gaining access to critical and sensitive areas of our daily lives. On the downside, such algorithms are brittle and vulnerable to malicious input, so-called adversarial examples. In these evasion attacks, a targeted input is perturbed by imperceptible amounts of noise to trigger misclassification of the victim's neural network. In this talk, we provide an overview of some recent results in this area, with a focus on adversarial attacks against automatic speech recognition systems. Furthermore, we will also sketch challenges for detecting deep fake images and similar kinds of artificially generated media.