Adversarial Machine Learning - the Coming Legal Storm - Abstract Only

Keywords— cyberspace, cyber law, jurisdiction, international law, private law, cyber definitions, autonomous malware, Internet

Abstract — The intersection of technology with the law always has been slow and often fraught with confusion. Lawyers do not speak the language of technology and, conversely, technologists are uniformly ignorant of the law's twists and turns. The purpose of this paper is to bring the legal community in closer tune with the technical community without forcing the legal community to undertake an in-depth education in machine learning (ML).

A key area of confusion is jurisdiction in cyberspace. There are, essentially, two camps. One side says that cyberspace is a domain of its own without laws, governance or enforcement. The other side claims that, in most cases international law as it stands is sufficient for managing legal aspects of the Internet.

The second is correct to a point. However, there are emerging areas of technology that appear to defy that position. One of the most dangerous and difficult – both theoretically and practically – is the area of autonomous malware. This paper discusses that challenge and proposes some approaches to meeting it.

We begin with some technical definitions and explanations to frame the legal issues properly in the technical world. We then address jurisdiction in cyberspace generally followed by demonstrating a standardized way of looking at the Internet through the lens of the law. Next we present a hypothetical attack of the type envisioned. Finally, we pose some possible solutions to the problem of autonomous malware and software-driven – as opposed to human-driven - attacks.

The full text version is available at *Legal Issues Journal* - https://www.legalissuesjournal.com/issue/082/