Ernesto Damiani
University of Milan, Italy

AI in Cyber Security

Abstract

Recent developments of artificial intelligence (AI) have already had a strong impact on cyber-security technologies. In security products today there is certainly no lack of examples of AI systems capable of extracting key elements from the information flows coming from the network and automatically channeling them to local and remote decision points. These systems are based on the idea of the "telescope", in which a periphery of passive sensors acquires all the information that it can find, and an intelligent system customizes and packages them for local reactions as well as that of remote decision center. A first generation of AI systems following the telescope approach has already demonstrated its potential in various security applications. However, attackers today have learnt to decouple malware infiltration, operation and exfiltration. "Sleeper modules" randomizing hostile activity along time make telescope-based detection more problematic. The second generation of AI systems for cybersecurity is still in a preliminary stage, but it is already leading to a radical change. AI makes it possible to conceive a "cyber-battlefield" composed of geo-space (the physical world), space (satellite and airborne detectors) and cyberspace where (i) humans may not be involved in tactical decisions, and (ii) the information proactively gathered by actions in a part of the environment is used to make automatic decisions (i.e., without going back up a chain of command) in another area. The talk provides an overview of the two generations of AI techniques for cybersecurity and points to some key aspects of the field's evolution.

Biosketch

Ernesto Damiani is the Senior Director of Artificial Intelligence and Intelligent Systems Institute, Khalifa University, leader of the Big Data area at Etisalat British Telecom Innovation Center, and Full Professor at Università degli Studi di Milano, where he leads the SESAR Lab. Ernesto Damiani's work has more than 15,500 citations on Google Scholar and more than 6,500 citations on Scopus. His areas of interest include Artificial Intelligence, Machine Learning, Big Data Analytics, Edge/Cloud security and performance, and cyber-physical systems. Ernesto has been a recipient of the Stephen Yau Award from the Service Society, of the Outstanding contributions Award from IFIP TC2, of the Chester-Sall Award from IEEE IES, and of a doctorate honoris causa from INSA – Lyon (France) for his contribution to Big Data teaching and research.