Artificial Intelligence Role in Cybersecurity Infrastructures

Cristian-Vlad OANCEA

Telekom Romania
oanceacristianvlad@hotmail.com

Abstract

The information technology domain advances and at the same time criminals are using new methods to commit cybercrimes. Cyber infrastructures are vulnerable to threats and other intrusions. Physical or virtual appliances and the human intervention are not sufficient for preventing, monitoring and protect all of these infrastructures. This situation implies a considerable automation and can be handled by applying methods of artificial intelligence that provide flexibility and learning capability for detection, prevention and combating cyber-attacks.

Index terms: Cybersecurity, Artificial Intelligence, Machine Learning, Cyber Threats, Cyberwarfare, Information Security

References:

[1]. P. Norvig, and S. Russell, Artificial Intelligence: Modern Approach. Prentice Hall, 2000.

[2]. E. Tyugu, Algorithms and Architectures of Artificial Intelligence, IOS Press. 2007.

[3]. Elon Musk Artificial Intelligence Mit (2015, Apr. 11) [Online] Available: http://www.businessinsider.com/elon-musk-artificial-intelligence-mit-2014-10?IR=T

[4]. Lynn Explains U.S. Cybersecurity Strategy, (2015, Apr. 19) [Online] Available: http://www.defense.gov/news/newsarticle.aspx?id=60869

[5]. Cybersecurity Fundamentals Study Guide, ISACA, 2014.

[6]. European Cybersecurity Implementation: Assurance, ISACA, 2014.

[7]. EU Cybersecurity Dashboard, A Path to a Secure European Cyberspace, Galexia, 2014.

[8]. T.J. Mowbray, Cybersecurity: Managing Systems, Conducting Testing and Investigating Intrusions, Thomas J. Mowbray, John Wiley & Sons Inc., 2014.