Artificial Intelligence in Shaping Preferences and Countering the Radicalization Process

Gary Kessler[1], Diane Maye[2] & Aaron Richman[3]

Embry Riddle Aeronautical University
Daytona Beach, FL U.S.A

TAM-C Intelligence
Philadelphia, PA U.S.A.

[1]kessleg1@erau.edu
[2]mayed@erau.edu
[3]arichman@tamcintel.com

Abstract*—This white paper suggests more research is needed in how Artificial Intelligence can shape preferences and decision-making, specifically regarding the radicalization process of violent extremists though the internet. We envision algorithm-based technology can be used to deter radicalization by influencing the user's preferences and decision-making outcomes.*

Keywords— **Artificial Intelligence, AI, preference model, decision analysis, social media, countering violent extremism, Project Maven**

I. INTRODUCTION

Terrorist groups such as the Islamic State have made unprecedented use of internet and social media tools to radicalize individuals and promote violent extremism. Terrorist groups can influence a decision maker's preferences and decision analysis through targeted branding and promotion of their ideology. To more effectively fight the Islamic State, in April 2017 the U.S. Department of Defense created an Algorithmic Warfare Cross-Functional Team known as Project Maven. Project Maven seeks to accelerate the integration of AI by automating the analysis of aerial surveillance captured by Unmanned Aerial Vehicles (commonly known as drones) over Iraq and Syria. Project Maven will also consolidate algorithm-based technology initiatives that "develop, employ, or field artificial intelligence, automation, machine learning, deep learning, and computer vision algorithms" (Work 2017). This paper suggests algorithm-based technologies should be explored in the context of deterring the radicalization process by influencing user preferences and decision-making through the social media and the internet.

II. LITERATURE SURVEY

The modern definition of Artificial Intelligence (AI) is "a rational and flexible agent that senses its environment and takes some action which maximizes its chance of success at some predetermined goal" (Alzahrani 2016). Notably, AI makes use of machine learning algorithms through a deep and complex neural nets. AI clusters data orders of magnitude beyond human capability which aids in disciplines such as criminal forensics and computer security. Additionally, web browsers such as Google and social media sights like Facebook have made use of AI to rank search preferences and conduct targeted advertising.

Similarly, online retailers such as Netflix and Amazon use algorithms to understand consumer preferences and suggest future purchases (Marr 2016).

Much of initial funding in AI came from the Defense Advanced Research Projects Agency (DARPA) (Buchanan 2005). Modern military applications of AI include equipment such as drones, the Gladiator Tactical UGV (used by US Marine Corps), ViPer (used by Israeli Forces), and the Talon (used for bomb-disposal) (Alzahrani 2016). AI seeks to produce computational artifacts that can help humans in [several] problems acting on their behalf; reasoning, explaining, learning and in general handling preferences are central issues to be tackled in any non-trivial artificial intelligence system" (Pigozzi, et. al. 2016).

In the context of decision-making, default preferences describe a decision maker's pre-existing preferences. In a 2016 study, Castelo, et.al. found "default effects are significantly enhanced when the intent of the choice architecture intervention is consistent with the preferences of the decision maker and when existing preferences are uncertain" (Castelo, et. al. 2016). Therefore, it is plausible a decision maker is more likely to change pre-existing preferences when presented with a new architecture.

III. PROPOSED WORK

In this study, we will start with how the adversary operates with regards to recruitment, propaganda, exploitation, and motivating individuals to conduct their next attack. In addition, we will assess how companies use branding and marketing algorithms to target consumer populations. There are programs currently in use that can assess these data points automatically after entering the specific parameters: both terror or intelligence analysts assess *pulse indicators* to understand what people associated with adversarial elements are expressing and their complete sentiment. The next step in this process would be to study the behaviors of these adversarial elements and create a typology to categorize them. For each category of behavior, researchers would develop a parallel response to counteract them with the intention for this parallel response to become automated in the future. Finally, the effectiveness of parallel responses must be measured; overtime more effective parallel responses will be used to counteract adversarial behavior. On a larger scale, effectiveness of the parallel response may actually mitigate radicalized recruitment.

REFERENCES

Alzahrani, H. 2016. Artificial Intelligence: Uses and Misuses. *Global Journal of Computer Science and Technology: Neural and Artificial Intelligence* 16(1): 11-15

Borum, R. 2011. Radicalization into violent extremism I: A review of social science theories. *Journal of Strategic Security*, 4(4), 7-36.

Buchanan, B.G., 2005. A (very) brief history of artificial intelligence. *Ai Magazine*, *26*(4): 53.

Castelo, N., et. al. 2016 Who Gets Nudged? How Choice Architecture Interventions Interact with Preferences.

Clark, J. 2015. "Google Turning Its Lucrative Web Search Over to AI Machines." *Bloomberg Business*. Bloomberg. Retrieved 17 May 2017.

Geng, B., Yang, L., Xu, C., Hua, X. 2012. "Ranking Model Adaptation for Domain-Specific Search," *IEEE Transactions on Systems knowledge and data engineering* 24(4).

Joachims, T. and Radlinski, F. 2007. "Search Engines That Learn from Implicit Feedback," *IEEE Computer Society* 40(8): 34-40.

Marr, B. 2016. "What is the Difference between Deep Learning, Machine Learning and AI?" Forbes. Retrieved 17 May 2017.

Pigozzi, G., Tsoukiàs, A. and Viappiani, P., 2016. Preferences in artificial intelligence. *Annals of Mathematics and Artificial Intelligence*, *77*(3-4): 361-401.

Riadi, I., et. al. 2012. Log Analysis Techniques Using Clustering in Network Forensics. International Journal of Computer Science and Information Security 10(7):

Salem, M., and Stolfo, S. 2010. Detecting masqueraders: A comparison of one-class bag-of-words user behavior modeling techniques. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications* 1(1): 3–13.

Sapkale, D., and Nair, P. 2016. An Improved Domain Classification of Google Search Results Using Naïve Bayes Classifier. *International Journal of Engineering Science and Computing* 6(7): 8592-8595.

Vedaldi, A. and Fulkerson, B., 2010, October. VLFeat: An open and portable library of computer vision algorithms. In *Proceedings of the 18th ACM international conference on Multimedia* (pp. 1469-1472). ACM

Weisgerber, M. 2017. The Pentagon's New Algorithmic Warfare Cell Gets Its First Mission: Hunt ISIS. *DefenseOne.* Retrieved 17 May 2017.

Wondracek, G., Holz, T., Kirda, E., and Kruegel, C. 2010. A practical attack to de-anonymize social network users. *IEEE Security and Privacy.*

Work, R. Memorandum for: See Distribution. Subject: Establishment of an Algorithmic Cross-Functional Team (Project Maven). U.S. Department of Defense. April 26, 2017.