RESEARCH AREA: Application of Culturally Augmented Machine Learning Models in the Analysis and Prediction of Advanced Persistent Threat Campaigns

G.Nowicki

The growing sophistication of existing and emerging cyber threats creates new challenges for defenders who rely on traditional methods of detection based solely on alert data. This applies especially to complex, multi-stage attacks carried out by Advanced Persistent Threat groups (APTs). The support these actors receive from nation states allows them to engage in long-term, resource-intensive campaigns. The progression of these attacks often follows a non-linear dynamic, which increases the difficulty of detection. It reveals the inadequacy of linear and correlative models that require more information than is often readily available as an attack progresses. Limiting the description of this complexity only to alert-data does not provide insight into the attack's lifecycle, or the attacker's goals and motives.

Recognizing the attacker's motivations and adapting their perspective allows the defenders to adjust countermeasures to the evolving threat landscape. A threat actor motivated by establishing presence for intelligence gathering will be motivated differently and use different techniques than one who believes their country is facing an existential threat. This perspective will also provide insight into the means that the attacker is ready to employ to accomplish their goals. Creating this visibility may be accomplished by incorporating cultural analysis into cyber threat intelligence.

Cyber operations that involve nation states are a realization of these nations' cyber and kinetic defense doctrines. These, in turn, are a reflection of the historical and cultural factors that shaped them. The set of measurable variables that approximate these cultural factors is based on tangible, cultural products such as political systems or various configurations of government administrations.

This research examines a method of incorporating the above described cultural factors into threat analysis by quantifying the regime type of sponsoring nation states and the index of democratic freedom. A Hidden Markov Model-based Machine Learning method was used to show how using culturally augmented alert data impacts the accuracy of attack prediction. The obtained results identified attack patterns that differ depending on the cultural variable included in the analysis. This research project is currently in progress and is aimed at developing a standardized methodology based on this approach.