## Research – Attacker Taxonomy

Research Question:

What are the dimensions of attacker cognition and socio-cultural identity for which effective defensive measures can be defined/implemented?

Attacker mental models can be usefully extended to understand dimensions of cognitive and socio-cultural susceptibility for exploitation and manipulation and to determine how these affect an attacker’s perception of qualitative and quantitative characteristics of cyber-attack surfaces. This would influence our understanding and implementation of effective defensive strategies, particularly those which may have an impact on attackers’ cognition.

These dimensions may include:

* Adaptability
  + Flexibility
  + Tolerance of chance
* Awareness of environmental change
* Tenacity
* Intentionality
* Cultural values/organizational structure
* Thinking ‘System 1 and 2’
* Opportunism vs. Directedness

**How do we measure dimensions of the attacker model?** Attacker cognitive and socio-cultural dimensions might be measured passively, derived from existing data (operational or experimental), or experimentally determined through direct manipulation of cyber environments. Future empirical research will be required, including human subjects’ experimentation.

**How well do we need to “know” the attacker for the model to have good utility?** The resulting taxonomy may have many measures. For an attacker type, subsets of the taxonomy and distributions of features across each measure might be useful for informing effective defensive strategies.

**How can we best use the attacker model to improve cyber defenses?** The attackers’ position with regard to each of these dimensions affects the nature and sophistication of the deceptive maneuver required, affecting the outcomes of carrying out an attack. For example:

* Force an attacker into System 1 thinking to exacerbate cognitive bias effects.
* Force an attacker into System 2 to slow down forward progress.
* Lure an attacker into using logical fallacies to inform bad heuristics.
* Induce specific cognitive biases to affect attacker behavior.
* Measuring an attacker’s susceptibility to specific cognitive biases.
* Using socio-cultural measures to determine attacker type or background.

Once an attacker model is defined, exploitation of this model may take several forms, including: use of defensive deception to misdirect an attack; implementation of oppositional human factors techniques to degrade the usability of specific attack tools and techniques; or more effectively engage with the attacker.

Research Approach:

1. Develop and validate an attacker taxonomy.
2. Investigate techniques for measuring cognitive and socio-cultural dimensions of cyber attackers.
3. Conduct experiments to evaluate the use of the taxonomy and associated measurements.
4. Exploit these measures to inform effective defensive strategy.