# Monterey Phoenix: A Modeling Approach to Cyber And Cryptology

Michael Collins, National Security Agency  Kristin Giammarco, Naval Postgraduate School

The National Security Agency, in partnership with the Naval Postgraduate School (NPS), offered a pilot virtual internship to cadets and midshipmen accepted into the NSA/CSS Service Academy Intern Program, the ROTC Cyberspace Intern Program, and selected students from the Senior Military Colleges. The virtual experience introduced modeling concepts which support computer-assisted reasoning methods critical to the national cyber and cryptologic mission. Topic areas included Enterprise Risk Management, Information Warfare, Human-Robot Teaming, Insider Threat, and Deception.

Each topic was guided by a subject matter expert. All of the groups used the NPS tool, Monterey Phoenix (MP), to model and assist them in studying real-world problems within the respective field. None of the students, and only two of the experts, had any prior experience with MP. All of the sessions were conducted in virtual meetings. Two weekly 1-2 hour sessions specific to the teaching and practice of modeling with MP were provided. Subject specific sessions were at the discretion of the subject matter experts.

MP is a user-friendly interactive tool for modeling behavior of complex systems. MP enables domain experts to define systems of systems behaviors linguistically in the language the experts use to discuss their area of expertise and interactively develop constraints using their own lexicon to validate and verify a finite state machine. MP is used to generate and then select event traces that comply with human intent for the process at hand. While all architects choose to include in the model expected behavior and choose specific behavior to exclude, MP allows one to probe the unexpected and unknown behavior. While MP enumerates the implied behavior of the specification through event traces, it demands the additional human cognitive engagement to assess the emergent behavior presented. That behavior in many cases can be unexpected in either positive or negative aspect depending on the real-world story explaining the viability of that scenario from different perspectives. In this sense, the discovery of unexpected emergent behavior in complex systems, MP provides computer-assisted reasoning. Often, this unexpected behavior is independent of implementation.

Exemplar outcomes of this effort are reflected from models within the Enterprise Risk Management team’s evaluation of posited Cyber attacks on jet fuel pipelines. One team studied the effects of such an event on the timeline of its supply chain. Via Gantt charts automatically drawn from the computed event traces, the impact on the availability of fuel could be assessed conditioned on the severity of the attack. A second team found surprising resiliency in the same supply chain based on unexpected behavior of those events that actually trigger investigations. Some cyber attacks considered would cause side-effect events which would trigger such actions but the side-effects themselves were never designed with the intent of detecting cyber attacks per se.

MP has truly interdisciplinary applications that benefits from the skills and insights related to all disciplines. The internship comprised 60 students participating from 15 universities representing a wide variety of STEM and non-STEM majors. The teams found 11 unexpected emergent behaviors, and identified a known "cycle" behavior pattern from Information Warfare that was immediately used by the Deception team to model a GOSSIP protocol, thereby simplifying the behavior description. It is very encouraging to see such a wide range of students with different academic interests and backgrounds applying MP with the ease they did to find relevant insights. The interactive use of formal schemas in a user-friendly and flexible expression of reasoning has shown significant progress in enhancing the rigor of architectural and high level analysis to capture human intent.