Human-Agent Teamwork for Cyber Sensemaking in Network Operations

Objective: A cyber sensemaking framework for network operations that embodies the principles of human-agent teamwork.

Human-Automation Teamwork with Agents, Policies, and Visualization

KAoS Policy Services and the VIA Cross-Layer Substrate: Ability to coordinate human-agent teamwork through dynamic, declarative, context-sensitive OWL policies.
Luna Agent Framework: Through integration with KAoS, the Luna Agent Framework supports teamwork properties. Optional state-based mobility allows dynamic optimization of computing resources.

Organic Resilience

- Resilience is achieved through (1) on demand creation of self-organizing capabilities for problem mitigation and recovery; (2) engaging the adaptive capabilities of humans.
- Organic resilience builds on a biological analogue (inter-cell signaling and differentiation) to enable agent self-organization.
- Collective obligation policies represent duties of a group of agents without specifying in advance who must do what.
- Properties enabling organic resilience include:
  - self-organization and adaptation at all levels, and including both analysts and agents.
  - plasticity and redundancy of agents and operations.
  - feedback cycles for agents and analysts that allow the ongoing evaluation and correction of operations.

The Flow Capacitor

- NetFlow "darts" travel downward through IPv4 space.
- Agents tag and visually highlight flows of interest.
- "Rings" constrain downward path of flows with specified properties.
- Multiple stacked planes allow exploration of complex questions.
- An infinite variety of types of planes is possible.

Coactive Emergence

- Coactive emergence describes the process whereby useful interpretations of data are created through the interplay of interdependent sensemaking activities by analysts and agents.
- First-order emergence of interpretive patterns arises from problem-space constraints currently expressed within policies and tool configurations.
- Second-order emergence arises from dynamic changes to the problem-space constraints by agents and analysts.

The CogLog and the Live Advisory

- The CogLog is a semantic Wiki-based tool prototype to aggregate agent and analyst findings.
- Agents can automatically "grab" pertinent data (e.g., IP addresses), enrich it through background research, and post it to the CogLog.
- The CogLog enables remote colleagues to view and replay the relevant data—and, potentially, launch protective actions.