**Title:** Cyber Intelligence Research Consortium Poster

**Authors:** McAllister /Jay

**Performing Organization:** Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213

**Availability:** Approved for public release, distribution unlimited.

**Supplementary Notes:** The original document contains color images.
Cyber Intelligence Research Consortium
Advancing the art and science of cyber intelligence

The Consortium is a member-funded initiative that researches and develops technical solutions and analytical practices to help people make better judgments and quicker decisions with cyber intelligence.

Consortium Offerings to Members
- **Steering Committee**: Guide Consortium activities and plan for future success
- **Cyber Threat Baseline**: Anonymized research of members’ cyber threat environments to identify common challenges and associated best practices
- **Tradecraft Labs**: Workshops to advance cyber intelligence capabilities and showcase relevant technologies
- **Implementation Frameworks**: How-to guides for navigating key analytical practices and technologies
- **Crisis Simulation**: Capture-the-flag exercise to apply analytical techniques and technologies to a simulated cyber attack
- **Intelligence Insights**: Biweekly emails and bimonthly newsletters on topics relevant to the practice of cyber intelligence

**Environmental Context**
Provides scope for the analytical effort
- Highlights the importance of context - technical and nontechnical, internal and external to an organization

**Reporting and Feedback**
Offers courses of action to enhance decision making
- Represents the communication of and subsequent responses to cyber intelligence
- Takes into account audience background and technical expertise

**Data Gathering**
Acquires and aligns data for analysis
- Asks the right questions to get the right data, and the right amount
- Relies on domain expertise (self and others) and technology

**Macroanalysis**
Assesses the strategic implications of a cyber issue
- Adds perspective, context, and depth
- Enables proactive and predictive intelligence
- Provides appropriate insight for technical and nontechnical audiences

**Microanalysis**
Assesses the functional implications of the cyber issue
- Examines the issue’s nature, ability, and quality
- Enables reactive intelligence

**Analytical Acumen**
Facilitates timely, actionable, and accurate intelligence on a cyber issue
- Conceptualizes an analyst’s interactions with the other components
- Represents analytical tradecraft—the ‘art’ and ‘science’ of doing cyber intelligence analysis

Contact: cyber-intel@sei.cmu.edu
twitter: @sei_etc

©2014 Software Engineering Institute

Consortium Conceptual Framework
Cyber intelligence: the acquisition and analysis of information to identify, track, and predict cyber capabilities, intentions, and activities to offer courses of action that enhance decision making.
This framework puts this definition into practice. It emphasizes the rigor, agility, and creativity needed to analyze threats in the complex and ever-changing cyber domain.