CYBER OPERATIONAL RISK TOOL (CORT)

CORT provides commanders situational awareness and understanding of mission-based risk assessment of the cyberspace domain to inform intelligence driven decisions

CORT
Cyber Operational Risk Tool

Cyber Operational Risk Tool, or CORT, is a research and development project that will provide the capability to ingest criticality, vulnerability and threat data, both automatically and manually, calculate risk to mission based on these attributes, and display all in views and a central risk dashboard. It provides a centralized capability to quickly identify critical systems that must be protected to ensure mission assurance and enable prioritization of limited cyber resources.

Priorities

- Models Critical Missions and Supporting Key Terrain – Cyber and Mission Relevant Terrain
- Highlights Mission Dependencies, Relationships, Vulnerabilities, and Threats by Cyberspace Domain Layer
- Provides Analysts the Capability to Perform Criticality Analysis, Risk Assessment and “What If” Simulation

U.S.ARMY

CORT

OVERVIEW

Cyber Operational Risk Tool, or CORT, is a government -off-the-shelf, or GOTS, tool that uniquely fills a gap not filled by any current GOTS or commercial-off-the-shelf, or COTS, tool. The initiative started as a proof of principle cyber mission assurance visualization software tool for the U.S. Army Materiel Command.

AMC provided the U.S. Army Space and Missile Defense Command an initial version of the tool and the command's Technical Center further expanded it into a dynamic operational risk tool, providing the calculus to visualize and enable situation awareness and provide a "so what" impact assessment to mission.

CONTRIBUTION TO CYBER DOMAIN SITUATIONAL AWARENESS

CORT models detailed critical mission decomposition and supporting key terrain–cyber and mission relevant terrain –cyber characterization; highlights critical mission/cyber dependencies and relationships; and visualizes emerging vulnerabilities, threats, gaps and seams by cyber domain layer.

- Enables risk to mission analysis and supports mitigation strategies informed by dynamic, interactive and customizable detail of cyberspace information.
- Denotes the depiction, perception and understanding of cyberspace as it pertains to a commander's operational environment and the correlating impact to critical missions, enabling mission assurance-based cyber threat analysis/intelligence and risk assessment.

TECHNICAL CONCEPT

CORT will be a web application utilizing an information system agile development strategy with development stratified in four-week incremental sprints further broken into epics and user stories. It is based on performance parameters and attributes for criticality analysis, risk assessment and visualization and provides the flexibility to leverage and incorporate rapidly evolving technology to ensure cyber situational awareness, risk assessment and mitigation capabilities remain viable through development, fielding and sustainment.

METRICS/MEASURE OF SUCCESS

CORT calculates and visualizes risk to critical missions and uses several existing Department of Defense models in its risk algorithm.

- Utilizes the U.S. Cyber Command Risk Assessment Model (vulnerability, threat, impact) to provide the overall framework for combining risk factors into a single value for deriving threat, vulnerability and impact from sub factors and applies math behind subjective risk sub factors.
- Utilizes the National Institute of Standards and Technology Special Publication 800-30 assessment scale (vulnerability, threat, impact) to provide conversion factors for qualitative to quantitative assessment ratings.
- Utilizes the Army Research Laboratory Security Control Assessor-Validator risk assessment process (vulnerability) to provide a mechanism for assessing vulnerability tied to existing severity valuations (e.g. Security Technical Implementation Guides) with correlating algorithms and formulas; and to provide a baseline for mitigations.
- Utilizes the U.S. Army Cyber Command Activity Capability Access Resources Expertise Model (threat) to provide a mechanism for assessing threat tied to threat indicators with G-2 community enhancements.
- Utilizes the SMDC Key Terrain–Cyber Mapping Methodology Model tactics techniques and procedures (impact/criticality) to provide criticality factors and mission impact metrics.

For more information, please contact:
USASMDC Public Affairs Office

P.O. Box 1500
Huntsville, AL 35807
Phone: 256-955-3887

www.smdc.army.mil
www.facebook.com/armysmdc
www.twitter.com/armysmdc
www.flickr.com/armysmdc
www.youtube.com/armysmdc

Distribution A 0519-01