

## TARA (Threat Assessment Risk Analysis) Management Framework

**TARA (Threat Assessment Risk Analysis) Management Framework** – We postulate that a quantitative, formal approach is needed for modeling system security, and proposed the outline of a refinement based approach that integrates security with other dimensions of security, reliability, survivability, and dependability. We describe the significance of the cyber security gap in terms of three dimensions (1) criticality, (2) threat and (3) vulnerability. We have increased criticality due to the emerging economic dependence on the Internet; increased threat, as a consequence of emerging global tensions coupled with an increased sophistication of perpetrators; increased vulnerability because of the increased pervasiveness of computing. Cyber security counter measures on the other hand are primarily defensive, qualitative and ad-hoc. Therefore, it is necessary to bring discipline to security management by providing a logic for specifying security requirements and verifying secure systems against such requirements. There is a need for managing system security by quantifying costs, risks, measures and counter-measures. TARA is based on the following premises:

- Enables us to formulate security requirements (imposed by a system's user), security goals (formulated by a system's designer/ architect), and security claims (formulated by a system's V& V team) in a uniform, unambiguous, coherent manner.
- Allows us to validate security requirements (do they reflect user needs?), verify security goals (are they consistent with security requirements?) and certify security claims (are they borne out by the implementation?).
- Allows us to dispatch security goals among various components of a system, and/or among various alternative methods (avoidance, detection, recovery, containment, etc).
- Allows us to manage security measures, in such a way as to maximize the impact of these measures (by checking for complementary, minimizing redundancies, etc).
- Allows us to combine security claims in a unified framework that supports formal / automatable reasoning.

The TARA tool is A *security specification* notation, which details how to capture security requirements of a system in a way that focuses on observable relevant effects rather than hypothetical causes; a *security abstraction* notation, which captures the security properties of a system; and a *security certification* formula, which formulates the condition under which a system (represented by its security abstraction) meets a given set of security requirements (represented by security specifications) . – Sheldon/Neergaard/Mili (NJIT)/Richardson

**POC:** Frederick Sheldon, PhD; Michael Neergaard, MS, Dave Richardson, BS  
Cyberspace Sciences & Information Intelligence Research (CSIIR) Group  
Oak Ridge National Laboratory P.O. Box 2008, Oak Ridge, TN 37831-6418  
[www.ioc.ornl.gov](http://www.ioc.ornl.gov)