

Survivability and Operational Readiness: Common Needs for Metrics and Assessment

Dr. John Alger, Deborah Bodeau, and Julie Connolly
The MITRE Corporation

Abstract

Enterprises that depend on information systems need ways to assess the survivability of those systems. National defense organizations need to assess their operational readiness, and increasingly their readiness with respect to information assurance. This position paper identifies needs for metrics and assessment methodologies that are common to the domains of Information Assurance operational readiness and survivability.

Background

In the traditional military, front line operational units must be “combat ready,” meaning the troops are ready to deploy, the aircraft are ready to fly, and the ships are ready to sail. A well established set of metrics and corresponding assessment approach exist to capture the operational readiness of these units. The role of Information Assurance (IA) in the combat arena is growing. Thus, the notion of combat or operational readiness needs to be expanded to accommodate this emerging domain.

The United States Department of Defense (DoD) definition of *Information Assurance* is:

Information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. (DODD S-3600.1)

While focused on information systems, Information Assurance involves ensuring that information-dependent functions can be performed correctly and in a timely manner.

Survivability is the property characterizing information systems that can continue to fulfill their missions in the presence of attacks, accidents, and failures. Thus, the survivability of information systems is a key component of IA operational readiness. Metrics and assessment techniques for survivability, if defined properly, can support IA operational readiness assessments.

At present, there is no well-defined process for determining whether or how well a nation or a national defense organization is prepared to sustain an IA attack. Similarly, there is no assessment-driven process for identifying organizational needs for IA resources, policies, and training. The lack of assessment techniques and metrics means that a national defense organization can determine neither its IA operational readiness posture nor whether its investments in technology, policy, and training have improved its IA posture.

Directions for the Development of IA Operational Readiness Metrics

Ultimately, Information Assurance Operational Readiness metrics must address IA-related capabilities of an *organization*: How well can that organization continue to perform its missions in the presence of attacks on information systems, on the information needed for correct and timely action, and on the personnel who use or maintain the information systems? A national defense organization must be able to assess IA Operational Readiness at varying levels of the organization, and (because cyberspace depends on physical constructs, such as communications media and the power grid) for different geographic regions.

However, assessment of an organization’s IA operational readiness will of necessity entail assessment of properties of its information systems, as used and maintained by its personnel. For instance, metrics for a system might include what percentage of known attacks system operators can detect, how long it takes system operators to detect an IA attack, and how long it takes for them to neutralize the attack. The latter two metrics can also be viewed as survivability metrics.

An assessment of an organization’s IA operational readiness requires identification of its missions, functions or activities, and the resources needed to perform those activities, and an assessment of the

criticality of the resources to different activities. In addition, an IA operational readiness assessment must identify, and determine the potential for impairing mission operations of, vulnerabilities in products, systems, and architectures. A variety of risk, vulnerability, and other analysis methodologies and tools enable such an identification and assessment. Examples include the Air Force's Vulnerability Assessment/Risk Management (VARM) methodology and tool and the Software Engineering Institute's (SEI's) Survivable Network Analysis (SNA) method.

While many of the information-gathering and analysis activities will be the same, IA operational readiness assessment has a somewhat different scope than risk, vulnerability, or network survivability analysis. It must be useful in conjunction with traditional operational readiness assessments. Thus, IA operational readiness must be assessed using a *set* of well-defined operational scenarios. In the military, different operational scenarios are defined at a minimum for peacetime, crisis, military, and humanitarian operations. Each operational scenario involves different assumptions about available personnel and resources, connectivity of military information systems to those belonging to other nations or non-governmental organizations, and reliance on critical infrastructures. Ordinarily, risk, vulnerability, and network survivability analyses involve developing a variety of specific threat or attack scenarios, but assume a single operational scenario.

In addition, IA operational readiness must be assessed for systems and organizations *as they are*. Risk mitigation is most cost-effective when applied early in the system life-cycle. Therefore, many analysis techniques are intended primarily for use during system design and integration.

Implications for Survivability Metrics

If properly defined, survivability metrics could be a central input to an overall IA operational readiness assessment. The definition of survivability metrics, and the accompanying assessment techniques, must address several questions:

- What does survival mean? Survivability is the capability of a system to fulfill its mission in a timely manner, even in the presence of attacks or failures. Thus, survival (and metrics for survivability) must be defined in terms of mission or operational requirements. A survivability assessment technique must enable the analyst to identify missions, and to link system capabilities and resources to those missions.
- Survive what? A survivability assessment technique must enable the analyst to describe an operational scenario or threat model, and to assess survivability in that context.
- Survive in what environment? A survivability assessment technique must enable the analyst to describe assumptions about the operational environment, and to assess survivability in that environment. It should facilitate changes to the assessment if the parameters of the operational scenario change. An assessment technique with a good "what-if" capability is desirable.
- Survive how well? Survivability, like operational readiness, is not an all-or-nothing proposition. A survivability assessment technique must enable the analyst to describe the level of capability that can be expected.
- Survive due to what? A system might survive an attack because of inherent robustness, or because an innovative system operator finds an effective work-around. A survivability assessment technique must enable the analyst to integrate assessments of operational, personnel, and technical capabilities.

The authors are undertaking an effort to develop a set of Information Assurance Operational Readiness metrics, as well as an approach for their collection and application, for use DoD-wide. Metrics in this context refers to measures that gauge an organization's ability to protect against, detect, and respond to IA attacks. Information Assurance is not a mature discipline, though, so these metrics may be more qualitative than those available to its traditional military counterparts. As a result, this effort will consider many different kinds of metrics and methods. Collectively, these metrics will be used to provide an overall organizational rating of IA operational readiness, as well as identify changes in resource allocation, policy, and/or training to *improve* IA operational readiness. These metrics will include or incorporate survivability metrics.