

Information Operations Red Team & Assessments™ (IORTA™)

fact sheet

Independent, objective system assessments to analyze, predict, improve design, train, make decisions about security options, and optimize program effectiveness

Assessments and red teaming are tools often used by decision makers in understanding their security risk, vulnerabilities, and defense posture. Yet it has been difficult to understand the value they have in managing efforts, answering questions, and making decisions. Is the task bounded correctly to be efficient? What kind of assessment is needed? Are they objective, complete, sound, reproducible, measurable, and most importantly, actionable? What is the quality? Furthermore, how is red teaming best integrated into a program?

These and other questions are addressed in red teaming and assessments performed by the IORTA program. Sandia National Laboratories has developed and continues to refine assessments of systems across a wide set of disciplines via the IORTA program. Based upon a 50-year Sandia history of assessments, and strengthened by multi-disciplinary technical programs across Sandia, IORTA takes advantage of a wide variety of assessment and red teaming techniques, tools, and facilities to optimize results on a variety of situations and systems throughout their lifecycle. We are committed to drive red teaming toward a science-based analysis and engineering tool. IORTA has been tasked to red teaming many systems and activities including:

- Research & Development
- Operational Systems
- Test & Evaluation
- Adversarial Modeling & Analysis
- C4I Architectures, Commands
- Methodology Development
- Exercises, Gaming, Planning
- Critical Infrastructures, SCADA
- Security Devices, Cryptography
- Opposition Force Exercises
- Corporate Espionage, Crime
- Experiments & Demonstrations
- World Event Analysis
- Training, Tool Development

We apply red teaming to a wide range of domains including cyber, physical, CBNRE, social engineering, mass perception, lifecycles, and system-of-systems. We refine our approach as needed with capability to reproducing a wide

Meeting National Security objectives to:

- Assess**
- Analyze**
- Predict**
- Decide**
- Train**



range of adversaries, considering sophistication, cultural issues, insider versus outsider, and technical ability.

Multiple Methodologies – Multiple Red Teams

One approach, technique, or methodology is often insufficient to answer the needs of decision makers. Similarly, one red team cannot maintain focus and expertise on all distinct issues. That is why IORTA is a family of red team programs that work independently or together to solve problems at hand. They share common resources and consider a spectrum of assessment methodologies and tools to meet the needs of each assessment and optimize results. A primary technique used is the IDART™ methodology, which is derived from IORTA's core red team component – Information Design Assurance Red Team™; however, IORTA utilizes other methodologies from within and outside of Sandia as required for a particular assessment. Even when the assessment does not call for red teaming, the IDART methodology and a malevolent adversarial view influence the process used to assess a system.



IDART is IORTA's Core Red Team



HSRT focuses on Homeland Security and Force Protection

The Right Team and Tools

In addition to multiple techniques, effective assessments require the right team and tools to obtain comprehensive answers about a system's vulnerabilities and security. A team is formed around a core group that understands IORTA assessment techniques and resources. They choose other members with appropriate expertise from around Sandia. Such matrixed members have honed skills in their disciplines for their own customers. This provides leading-edge expertise for the assessment. Such team composition adds significant value for our customers.

The resulting teams are refined with appropriate tactical training on technique, technologies, and environmental knowledge. It is also enabled with other IORTA tools including specific methodologies, databases, libraries, attack resource labs, software applications, hardware systems, and project management staff. IORTA's techniques are refined through internal and external R&D. An important tool is adversarial modeling, which is required to generate measurable, consistent results in various IORTA's red teaming efforts. In efforts focused at understanding or predicting adversarial intent and behavior, it becomes critical to the success of a red team effort. A spectrum of outsiders and insiders can be considered. IORTA's training program is a tool used both internally for improvement of assessments and also externally for some agencies and groups. Training includes both methodology and technical focus from a malevolent adversarial point of view.

Information Operations (IO)

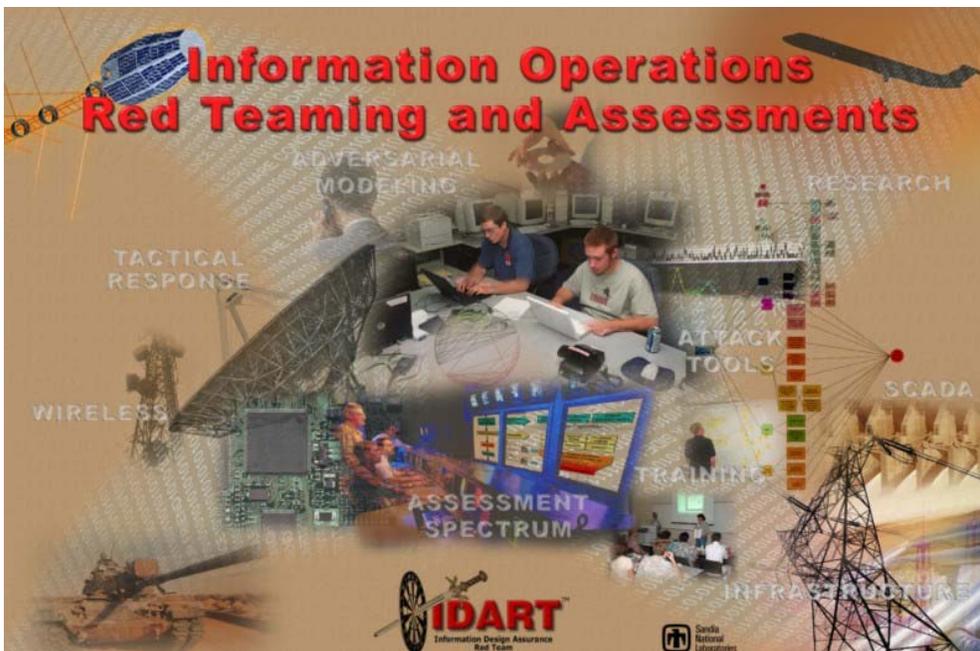
In addition to cyber-induced effects on transmission of digital signals, IORTA considers system information effects including those induced by attack through means such as physical, electronic, human perception, social engineering, psychological operations, human factors, and system interdependencies. Such efforts are augmented by Sandia's capabilities and test facilities in these disciplines.

Assessment Activities, T&E, R&D

IORTA has assessed systems, situations, and organizations for U.S. and local government, military, industry, and critical infrastructure providers. We have also used red teaming to perform and augment test and evaluation functions for our customers. Critical infrastructure systems IORTA has assessed include:

- Electric Generation & Transmission
- Banking & Finance
- Water (local & supply)
- Oil & Gas
- Telecommunications
- Transportation

IORTA engages in research and development to advance assessment science and tools through internal and externally funded research programs. Collaborations with government, industry, universities, and other government red teams are also pursued. We host an annual REDTEAM Conference for government-related red teams and customers of red teaming to help advance the discipline. Additional information is available on the IORTA web site.



For more information, contact:

Michael Skroch, Manager
Information Operations Red Team
& Assessments (IORTA)
Sandia National Laboratories
P.O. Box 5800; MS 0671
Albuquerque, NM 87185-0671
Phone: (505) 844-0104
e-mail: mjskroc@sandia.gov

web: www.sandia.gov/iorta/

web: www.sandia.gov/idart/