OFFENSIVE & DEFENSIVE CYBER
PLUS INFORMATION OPERATIONS

From replicating social media environments that facilitate enemy operations to delivering nation-state intelligence, surveillance, and reconnaissance of mission-critical infrastructure, SMEIR prepares our nation's military with multi-domain training and intelligence.

WEBSITE & SOCIAL MEDIA REPLICATION

Realistic replication of hostile networks, social media, local and host nation government, international, regional and local news websites, insurgent crowdsource funding pages, and deep web.

VIRTUALIZED NETWORKS

Dragging and dropping network components into blueprint models, with customizable attributes and pressing play, ensures the training environment is automated, innovative and scalable.

EXERCISE DEVELOPMENT & MANAGEMENT

Development of cyberspace scenarios to meet exercise objectives. SMEIR integrates sentiment and white noise into a variety of scenarios, each agile and capable of scale.

MALICIOUS TRAFFIC GENERATOR

Whether running automated cyber threats or penetration testing security vulnerabilities, IDS can integrate offensive and defensive cyber attacks for replication in live operational environments.

SUBJECT MATTER EXPERTS

IDS can provide training technical support, cyber range exercise conduct assistance, serve in an advisory role, and/or assist with scenario evaluation as requested.

CONTACT US: 703.875.2212 or cyber@idsinternational.com
www.smeir.net

IDS INTERNATIONAL