

# FORCYTE

Cyber Situational Understanding

ENABLING STRATEGIC DECISION MAKING

Forcyte is an exportable Cyber Situational Understanding & Awareness tool designed to provide Visualization of the Cyberspace and Electromagnetic (CEMA) domains, Planning & Mission Management and Intelligence-driven Operations.

It is built on a modular design and open framework that is operationally tested, and leverages standards such as the Structured Threat Information Exchange (STIX) and Trusted Automated eXchange of Indicator Information (TAXII) for Threat Intelligence.

Forcyte utilizes mission playbooks, workflows, standard military symbology, and user roles mapped to Joint Doctrine, enabling familiarity and ease of use.

### Cyber Situational Awareness

Provides Awareness and Understanding of impact to mission and associated response options to drive actionable mission outcomes.

### Cyber Planning and Mission Management

Mission Plans, Playbooks, Plays and Courses of Action are modelled and missions may be simulated for training exercises, or operationally executed.

### Cyber Survivability Assessments

Provides a key element for simulated force-on-force survivability assessment with Measures of Effectiveness, Measures of Performance (MOE/MOP) and post-execution analysis.

### Operationally Tested

Field tested with integrations to many military systems, commercial products and compatible with the US Army Common Operating Environment (COE).

## APPLICATION FRAMEWORK



Widget Dashboard



Cyberspace Visualization



Mission Management



Cyberspace Intelligence

## FOUNDATIONAL COMPONENTS



IMSEA API



IMSEA Engine



Common Graph Model



Forcyte Core



Auto Net Map

### Plugin Architecture

Cyber Sensor Data

Cyber Intel Data

Cyber Terrain Data

Operational Data

- + Open Architecture
- + Modular Design
- + Customizable Dashboards
- + Mission Workflows
- + Enhanced Visualization
- + Threat Playbooks

- + Forcyte is specifically designed to support the planning, execution, and monitoring of cyberspace operations

## Key Features

### Cyberspace Threat Intelligence Editor

- Enables network defenders and intelligence analysts to send, receive, and edit STIX data.
- Link diagrams of cyber attacks and machine-readable graphs may be shared to help others defend against similar attacks.

### Order of Battle Editor

- Visualizes the task organization and associated capabilities of friendly, neutral and enemy forces in an easy-to-navigate tree structure.

### Mission Planning and Management

- Supports mission planning for multi-domain missions.
- Provides mission rehearsal and simulation capabilities with real-time health & status monitoring of mission execution.

### Cognitive Engine Catalog

- Creates custom analytics to alleviate cognitive burden.
- Enables junior-level operators to create complex analytics without requiring intensive data science training.

## Cyberspace Domain Visualization

### Cyber-Physical View

- Geospatial overlay to present infrastructure, sites, and units
- Provides overview of network device location, health and status
- Context-aware pivoting between views

### Cyber-Logical View

- Shows network topology for cyber terrain
- Blue, Red, and Grey cyber terrain
- Spectrum dependent devices and RF connection types
- Multiple security enclaves
- Physical vs Logical connections

### Cyber-Persona View

- Shows relevant personas of interest
- Blue, Red, and Grey personas
- Display alerts from user behaviour cyber sensors
- Tracks enemy personas from social media accounts, system logins, email accounts, etc

Forcyte uses "Cognitive Engines" that make use of the Observe, Orient, Decide, and Act (OODA) construct to model an analyst's thought process. The system will **Observe** streaming data, **Orient** the data by providing context using the Common Knowledge Graph to assess impact, **Decide** which actions to recommend to the user, and even **Act** on the recommendations in a fully autonomous manner.

Forcyte takes all of the data inputs and contextualizes them in the **Common Knowledge Graph** that uses a Semantically-Enabled Ontology AI technique to understand the relationships between the complex data.

Forcyte **receives data** that has been processed by cyber sensors, log aggregators, and other operational Programs of Record.

