twoSIX TECHNOLOGIES

Two Six Technologies

IARPA BENGAL Proposers Day

TWOSIXTECH.COM

Suite of Products

STRATEGIC ADVANTAGE: PLATFORMS FOR SOFTWARE DELIVERY

IKE

Cyberwarfare platform utilizing machine learning and AI to improve human understanding of the digital battlefield.

PULSE

Platform for full spectrum operations in the information environment, including persistent passive data collection, multi-platform audience engagement, and custom data views and dashboards.

M3

Media Manipulation Monitor (M3) detects and analyzes media manipulation by foreign governments, including censorship, disinformation, and propaganda campaigns.

SIGMA™

Region-scale CBRN platform (Chemical, Biological, Radiological, and Nuclear) for real-time detection, identification, and response.

TrustedKeep™
SECURITY PLATFORM

Comprehensive security platform that implements Zero Trust data protections and provides object-level encryption for sensitive data at scale.

Technical Areas of Expertise

Deep expertise in five focus areas enables Two Six to deliver impact focused innovation at speed

CYBER

Comprehensive cyber capabilities, including network security, CNO, AI vulnerability research, cryptography, and all-domain digital battlespace

ELECTRONIC SYSTEMS

Specialized expertise in embedded device security, hardware and firmware vulnerability assessments, reverse engineering, microelectronics, and FPGAs and custom PCB design

SECURE SOLUTIONS

Scalable object-level encryption and enterprise-grade protections for the most sensitive data, in the cloud, on-premise or in hybrid environments

INFORMATION OPERATIONS

Our platforms enable listening, discovery, and engagement, and help to identify and counter misinformation and propaganda in the information environment

ANALYTICS

Data analytics and visualizations provide powerful insight into the most complex data sets

Talented teams with unique expertise and dedicated specialists
Highly respected centers of excellence within each focus area

Transitions from R&D to Mission Impact

Two Six Technologies rapidly transforms theoretical concepts into operational solutions and scalable products to solve Customers' challenges

R&D

Strategically focused R&D efforts

Long, deep relationship with DARPA and other R&D partners

Performance on 75+ historical projects of sponsored research

Alignment of R&D activities within the 5 focus areas

R&D teams embedded within operational business units; maintain focus on Customers and Missions

World-class teams of researchers, scientists, and specialized experts

TRANSITIONS

Strategic objective to transition R&D projects to prototypes, fielded systems, and operational solutions

Deliver innovative technology into the hands of warfighters and end users; avoid "science projects" or delivery to "a shelf in DARPA's basement"

Team of field engineers support operational customers

Dedicated team of UI / UX experts to facilitate adoption by end users

Productized solutions for government and commercial customers

CASE STUDY IKE

Proven ability to transition technology

Leverage R&D innovations, cyber expertise, operational experience, and strategic focus on customer missions

From origins as a DARPA R&D project, now IKE is operationally deployed with U.S. Cyber Command and established as PoR for JCC2

Strategic coordination to generate R&D breakthroughs, rapid prototypes, and successful transitions of practical technology into the hands of warfighters and end users

TST Expertise

- Adversarial ML
- AI Risk Management Frameworks
- Computational Social Science
- LLM Fine Tuning
- LLM Threat Assessment
- Syntactic & Semantic Parsing
- Dis/Misinformation Detection
- Formal Methods
- Secure System Design
- Software Development

Complementary

- Specific LLM Attacks
- Prompt Injection
- Information Retrieval

ARMORY

- An extensible platform for evaluating the robustness of AI models to adversarial attacks
- Open source: https://github.com/twosixlabs/armory-library
- Evasion and poisoning attacks against a range of model types/tasks, including:
  - Object detection, image classification, multi-object tracking, audio ASR, speaker ID, and multi-modal classification (EO+SAR)
- Baseline datasets, models, and attacks provided; can be extended

LLM Risk Assessment Tool

- LLMs have known weaknesses.
- Assess via NIST AI RMF
  - **Map** the known risks mission needs
  - **Measure** the effect of weakness on mission success
  - **Mitigate** adverse effects:
    - Adopt different models, Human in the Loop, Reduce Reliance, etc.
  - **Manage** deployment risk by tracking deployment data

Known Vulnerability	Technical Documentation	Social Network Surveillance	Secure code production
Wrong or outdated information	✓	✗	✓
Vulnerable/ erroneous code production	✗	✓	✗
Weak cross cultural understanding	✓	✗	✓

TST Personnel and Facilities

- 600 employees, 80% cleared TS or above.
- Headquartered in Arlington, VA with offices in 8 cities across the U.S.
- TOP SECRET facility clearance with approval for TOP SECRET storage and multiple classified AIS, COMSEC, ALC, SAV, and DARPA Secret Wide Area Network (DSWAN) systems.