



a PARSONS Company

the Future of Information Dominance

Operationalizing Information Advantage

*Advanced Training & Technologies
for
Front Line Operators in the Information Environment*

This proposal includes data that will not be disclosed outside the Government and will not be duplicated, used, or disclosed—in whole or in part—for any purpose other than to evaluate this proposal. If, however, a Contractor is awarded to this offeror as a result of—or in connection with—the submission of this data, the Government will have the right to duplicate, use, or disclose the data to the extent provided in the resulting contract. This restriction does not limit the Government's right to use information contained in this data if it is obtained from another source without restriction.

Relooking our Strategy for Influence & Operations in the Info Environment

Many generations of Americans have lived and enjoyed the power and dominance our nation has secured, particularly in the land, air, and maritime domains. But today's battlespace has significantly changed with revolutionary advancements in cyber, EW and space-based capabilities. The adversary has demonstrated highly adept capabilities and capacity to conduct Operations, Actions and Activities (OAA) discreetly within the Physical and Informational Environments and to influence behaviors, activities, and outcomes often before the US military's OODA loop has had a chance to react. In today's 21st century battleground arena – known as Great Power Competition – information is king, and for the nation who obtains information advantage, shall undeniably maintain the overall advantage.

For decades, our strategy has been deterrence through posture and forward presence – focused on clearly demonstrating to our adversaries a sustained readiness and willingness to “*fight tonight*”. Deterrence may be helpful to maintaining partnerships and alliances, but it has been virtually ineffective in modifying the behavior of China and Russia who are waging 21st war now – albeit by another means. These adversaries have learned to compete on a day-to-day basis, utilizing a broad array of government, commercial, and private tools, and techniques without breaking the threshold of armed conflict. They are adept in operating below the threshold of armed conflict and at the fringes of international laws. Their OAA are employed discreetly through Political, Military, Economic, Social, Information, Infrastructure, Physical, and Time (PMESII-PT) factors. Across this vast PMESII-PT continuum, Information is THE common denominator and THE most influential domain of all. For the behaviors and decisions of individuals, groups and nation-states are formed and informed by human cognition and biases which are all based on the information being received and transmitted within relative environments.

With this fundamental understanding and appreciation of the criticality of information, 21st century military organizations must operationalize information advantage by properly training and equipping its personnel with advanced techniques and technologies in strategic communications, psychological operations, virtual persona operations, cyber operations, electronic warfare, and space operations. Parsons Corporation firmly believes that in order to regain the initiative and dominate in 21st century competition, the Department of Defense must prioritize innovative training and cutting-edge technologies for full-spectrum operations in the Information Environment (OIE). Parsons maintains a broad inventory of seasoned experts and industry-leading technologies to provide best-of-breed training and equipping for Virtual Operations in the Cyber Domain as well as full spectrum Operational and Intelligence Preparation of the Environment (PE).

Our people are our most precious asset. Ensuring that they have the best training and equipment to conduct effective OIE is how we effectively Operationalize Information Advantage.

OIE Training, Readiness and Technology Solutions for Today and Tomorrow

Parsons' suite of holistic training and readiness solutions to Operationalize Information Advantage are focused on delivering commercial best practices to understand and exploit the Information Environment (IE) with advanced tactics, techniques and procedures. Information operations (IO) and cyber-persona effects are only effective if they can achieve overmatch against the IE platforms, user community and our adversaries. Pivots are occurring in the IE – Commercial Platform fraud detection is better; adversaries are increasingly intertwined with global social media platforms and users; deep fake technologies are becoming more and more elaborate and difficult to detect.

Parsons is in the business of equipping DoD with the necessary skills and tools to safely understand the digital environment in a manner that allows both organizations to remain and sustain a step ahead of the threat attempting to cause harm to your personnel, reputation, brand, assets, network and supply chain. Parsons will assist in curating data and building tools that guide targeted interventions. We will do this collaboratively, working with existing efforts and sharing best practices as we go. The solution will safely discover, synthesize, and analyze publicly available data and metadata to provide actionable insights for more effective decision-making. Solutions are conducted in a digitally immersive environment and utilize a flexible framework and methodology that is driven by and centered around your enterprise requirements. Some of our clients include Fortune 1000 companies, a Fortune 100 company, a Fortune 400 company, several universities, and elite Special Operations units supporting countless missions and skill identifiers. Parsons provides solutions that adhere to privacy and data protection laws and principles. Parsons protects privacy while taking advantage of the potential of digital technology to maximize the speed and real-time capability of national pandemic responses. Our goal is to make this technology available to all operators, leaders, and subordinates alike, as quickly and seamlessly as possible.

Parsons has over a decade of experience providing training and technical support on Virtual Operations and Open-Source Intelligence (OSINT) collections and activities for DoD and Intelligence Community (IC) partners. Our Virtual Operations training teaches students how to create, build and employ sustainable digital personas to support and advance an organization's objectives and activities in the cyber domain. Our OSINT training and support includes data analysis and exploitation, tradecraft development, and technology development to support OIE.

Our Suite of Advanced Curricula

Our **Virtual Operations Training Course (VOTC)** teaches students how to create, build, and use digital personas to support and advance an organization's virtual operations program. The one-week course begins by walking students through the step-by-step process of how to create and build a digital persona, then focuses on how to use personas online, and ends with a series of exercises that test the students on their ability to use the personas in a real-world operational scenario. This immersive and hands-on course is designed to prepare students so they can return to their organization with the skills needed to use personas to advance their support their organization's missions.

Differentiators

- Based on best-in-class curriculum that translates to mission outcomes
- Instructors with 200+ years combined experience & lessons-learned from more than 2000 graduates
- Holistic, skills-based, and tool-agnostic training tailored to your needs
- Train at the speed of technology - learn with real-time and relevant data
- Delivered locally or as a mobile training team

Our **Cyber Advanced Support Operations (CASO™)** training teaches students an iterative discovery, assessment, and analysis framework that can be applied with the use of various tools and methods to make sense of open-source data to include academic journals, foreign news media, social media, and other web-based sources. Our cutting-edge best practices have proven success in facilitating creative problem solving, reducing research cycle times, and honing analytical skills to see what others cannot see. We instruct the same framework throughout every course regardless of areas of interest or the utilization of open source, moderate, or expensive technologies and tools.

Students are equipped with the necessary skills to safely operate on the internet, protecting identity and related digital footprint, while simultaneously establishing a new frame of reference for undertaking digital PE research. Students will leave the course with the ability to implement newly learned skills at their respective organizations, provide active support to organizational requirements, tip and cue critical information to exquisite systems, and produce more effective research deliverables that provide meaningful context and information for stakeholders. The fluid and complex nature of the digital environment demands a knowledge worker-based discipline in Operations Security (OPSEC), Military Information Support Operations (MISO), and Military Deception (MILDEC). DoD operators learn how to navigate and influence a dynamic and ever-changing environment vice static classroom lectures and rote memorization.

Parsons has experience providing Geospatial Intelligence (GEOINT) analysis and support to Department of Defense (DoD) and IC customers. This experience includes analyzing, assessing, and exploiting geospatial information to describe, assess, and visually depict the operational environment for our customers. For example, Parsons utilized multiple geospatial analysis tools (Esri, FADE/MIST, OpenIO, etc.) to discover and analysis geospatial information that includes all-source information, OSINT, SIGINT, MASINT, and IMINT. We have experience supporting Special Operations, Geographic Combatant Commands (GCCs), and the IC (including NGA) with geospatial analysis. We also provide geospatial data exploitation, validation, and fusion across multiple INTs using COTS and GOTS tools, as well as artificial intelligence and machine learning. Our end product analysis typically consists of intelligence reports that provide contextual geospatial analysis to understand events, areas of interest, patterns of life, and information operations within a geographic region.

Parsons has undertaken research and development of specialized geolocation capabilities that fall within the GEOINT domain. For our applications, our design concepts have included RF direction-finding (DF) and emitter geolocation using software-defined radio (SDR) based platforms and advanced digital signal processing (DSP) algorithms to autonomously detect and geolocate multiple HF/UHF/VHF transmitters simultaneously. Our design allows systems to be networked together to provide greater area coverage and more precise triangulation of threat emitters. Tactical signal monitoring and DF systems in use today are mainly "scanning" systems that use a single channel to search against a known frequency list and, upon detection, trigger narrowband tuners in an antenna array for DF processing. The Parsons design is aimed at detecting and direction-finding all HF/UHF/VHF frequencies simultaneously. The operator does not need to scan through pre-program frequencies and "chase" signals of interest.

Our **Commercial Signature Reduction (CSR)** courses utilize hands-on practical scenarios and instruction on various methods, techniques and tradecraft where learning new skills is the focus, as

opposed to the technology or tool. The CSR curriculum is uniquely designed to provide students with cutting edge best practices that have proven success in facilitating creative problem solving, reducing digital exposure, and honing SIGREDUX skills to mitigate what others can see. CSR teaches students a comprehensive SIGREDUX methodology that can be applied with the use of various tools and applications to protect both personal, professional, and operational information. Students graduate the course with the skills to effectively mitigate spillage of sensitive information.

Our **CONVERGENCE Program** is designed to teach operators an active-detect posture while tackling issues like identifying, understanding, and mitigating foreign influence using online social media, news outlets, and other internet-based domains. CONVERGENCE serves as a framework for creating and managing training conducted in the IE and to support development of information related capabilities. The fluid and complex nature of the digital environment demands a knowledge worker-based discipline in Operations Security (OPSEC), Military Information Support Operations (MISO), Military Deception (MILDEC) and Deception in Support of Operations (DISO). Operators need to learn how to operate in a dynamic and ever-changing environment vice static classroom lectures and rote memorization. Our tool-agnostic research methodology allows the operator to pivot from globally disbursed virtual populations to onsite atmospherics and corroborate and validate information, improving cross-cultural agility by leveraging technology.

Our suite of technologies and commitment to the mission

Parsons provides innovative technology-driven solutions to afford participants the freedom and security to navigate contentious SIGINT and Cyberspace domains. By employing a Full Spectrum Radio Frequency, Cellular, Wi-Fi, Bluetooth & GPS *'monitor, intercept and defeat package'* we place a special emphasis on low-vis passive / semi-passive collection aimed at illuminating all Commercial Signatures (e.g., cell phones, smart watches, push-to-talk radios). Additionally, we provide subject matter expertise in the disciplines of tactical SIGINT, Cyber, and CEMA (Cyber-Electro Magnetic Activities) operations with the desired outcome of enabling the US SOF operator through recommendations to reduce both MILSPEC Communications Signatures & Commercial Digital Signatures.

Parsons' Virtual Persona Operations technology and tradecraft support realistic, persistent and survivable online activities in the IE to enable our service members to own the information advantage. Our managed attribution suite of services known as Dimensions, Digitz, Omega and Inception enable IO professionals to conduct the following advanced activities:

- Virtualized mobile comms Point of Presence w/2-factor authentication on true cellular infrastructure
- Remote and virtual control of real mobile devices
- Persistent and dedicated mobile IP presence and mobile network data
- Regional diversification of IP ranges and locations worldwide
- Diversified virtual environments tailored to specific needs, software or OS
- Scalability to support rapid operational growth as needed
- Interactive user functionality, including file transfer and CAPTCHA defeat

Parsons stands ready to assist our DoD operators and will continue to build on achievements and lessons learned to effectively serve in the nation to deter our adversary, assist and engage with U.S. partners and allies, and to prepare and shape the environment. Parsons partnered with the right DoD

organizations to train and equip our service members with the right techniques and technologies will ensure new concepts and new curriculum and ensure sustained advantage in 21st century multi-domain operations.

Parsons stands ready to contribute training, technology and innovation in support of Operationalizing Information Advantage across the force to ensure we continue to dominate in competition around the globe.