103 Quality Circle, NW
Suite 220
Huntsville, AL 35806

SCIENTIFIC RESEARCH CORPORATION

August 2023

Enabling a Data-Centric Army

SRC's Capabilities in Cyber and Intelligence Operations

CONFERENCE WHITE PAPER

Armed Forces Communications & Electronics Association International (AFCEA) TechNet Conference – Augusta 2023

Introduction

In the continuously-evolving military and defense operations landscape, a data-centric approach has emerged as a critical strategy to enhance efficiency, effectiveness, and success within the cyber domain. Scientific Research Corporation (SRC) offers cyber and intelligence operations capabilities that support the data-centric strategy needed to meet emerging challenges faced by the U.S. Government and defense industry.

The Armed Forces Communications & Electronics Association International (AFCEA) TechNet Augusta 2023 conference focus is to explore how data-centric methodologies empower military forces to leverage vast amounts of information to their advantage. SRC's expertise aligns with the conference theme, as the company's contributions enable the transformation of its customers into a data-centric force, driving progress and success in an era of information-centric warfare.

This document provides an overview of SRC’s capabilities and its significant contributions in providing innovative solutions to its customers.

Background

The data-centric approach has transformed the modern military landscape, revolutionizing military operations by offering several key advantages which include:

Informed Decision-Making:

Access to real-time and historical data enables military leaders to make well-informed decisions, optimizing strategies to maximize the chances of mission success while minimizing risks. By leveraging data analytics and intelligence, decision-makers can gain valuable insights into various aspects of a mission, such as threat assessment, troop movements, logistics, and resource allocation.

Improved Situational Awareness:

With data streams from various sensors, satellites, and reconnaissance assets, military personnel can have an up-to-date and accurate picture of the battlespace. Enhanced situational awareness allows for timely responses to changing circumstances, giving the military a critical edge in combat situations.

Precision Targeting and Engagement:

Advanced data analytics enable precise targeting of enemy assets and threats. By analyzing patterns and trends in data, military forces can identify high-value targets, predict potential enemy movements, and execute surgical strikes with reduced collateral damage.

Predictive Maintenance:

Utilizing data from sensors and equipment status monitoring systems allows for predictive maintenance of military hardware. By identifying potential faults or performance issues in advance, parts can be sourced and maintenance can be

scheduled proactively, reducing downtime, and increasing the overall readiness of military assets.

Cybersecurity and Information Assurance:

Robust cybersecurity measures are essential for safeguarding sensitive military information, networks, and equipment from cyber threats. Utilizing data analytics and machine learning, security professionals can detect, deny and respond to cyberattacks more effectively, protecting critical data, communications, and infrastructure.

Continuous Learning and Improvement:

Data-driven operations promote a culture of continuous learning and improvement within the military. By collecting and analyzing data from past missions and exercises, the military can identify areas for enhancement and adjust tactics and strategies accordingly. This process helps ensure that the armed forces remain adaptable and can respond effectively to evolving threats.

Artificial Intelligence (AI) and Autonomous Systems:

The success of AI-driven solutions relies heavily on data. A data-centric approach provides the foundation for training AI algorithms and enabling autonomous systems. These technologies can augment human decision-making and improve overall operational capabilities by providing insight into information gaps, data discrepancies, and analysis of data sets.

Adopting a data-centric approach in military and defense operations is not only crucial, but increasingly necessary, as the landscape of modern warfare is continuously shifting. The utilization of data analytics, AI, and advanced technologies empowers military forces to make better decisions, increase efficiency, and maintain a competitive advantage on the battlefield, ultimately contributing to the success and safety of military operations and defense of the U.S.

SRC's Cyber and Intelligence Operations Support

SRC plays a critical role in supporting cyber and intelligence-related programs for the Department of Defense (DoD) and other U.S. Government agencies. SRC's expertise encompasses a wide range of capabilities that are instrumental in enabling a data-centric army.

Intelligence Operations Support:

SRC's intelligence analysts play a vital role in supporting cyber operations by analyzing classified and unclassified data for U.S. Armed Forces' cyber operators. The intelligence analysts provide threat intelligence assessments, conduct All-Source Intelligence Research, and offer real-time analysis of data during exercises. This intelligence-driven approach empowers the military to make data-centric decisions, optimize cyber defense strategies, and prioritize resources based on the most critical

threats. The intelligence analysts' valuable insights into cyber threat patterns, adversary behaviors, and potential vulnerabilities enhance the U.S. Armed Forces' cyber readiness.

Cyber Operations Support:
SRC manages and operates classified and unclassified cyber ranges that provide specialized and controlled environments designed to simulate real-world cyber scenarios. These cyber ranges serve as crucial facilities for developing, honing, and validating cyber capabilities, tactics, and defensive strategies for cybersecurity military personnel and hardening cyber equipment, networks, and systems. The ranges allow for comprehensive cybersecurity training, test and evaluation, and research activities, affording users hands-on experience in tackling diverse and complex cyber challenges. By utilizing classified and unclassified environments in these exercises, the U.S. Armed Forces can improve its cyber situational awareness and enhance its cyber defense and response capabilities.

SRC's Data-Centric Solutions

SRC's capabilities are designed to support and enhance military operations within the cyber domain. Such capabilities include:

- Management and operation of cyber ranges
- Cyber intelligence analysis
- Synthetic persona development
- Cyber range environment development

Management and Operations of Cyber Ranges:
SRC's provision of classified and unclassified cyber ranges enable the U.S. Armed Forces to conduct realistic and comprehensive cyber training exercises. SRC models its cyber ranges to simulate real-world environments and adversaries, yielding actionable data that allows military personnel to analyze and respond to various cyber threats and scenarios.

SRC-managed cyber ranges offer a secure and controlled setting where military personnel can hone their cyber skills and strategies. By utilizing simulations and scenarios in these cyber range environments, the U.S. Armed Forces can assess its capabilities, identify vulnerabilities, enhance training curricula, and develop data-centric approaches to cyber operations.

Cyber Intelligence Analysis:
SRC's cyber intelligence analysis capabilities are central to enabling a data-centric army. By analyzing both classified and unclassified data, SRC's intelligence analysts

provide valuable insights into potential cyber threats and adversary tactics. This threat intelligence empowers the U.S. Armed Forces to make informed decisions based on assessments of cyber risks. Additionally, real-time data analysis during exercises allows military personnel to adapt quickly to evolving cyber threats, making their operations more agile and effective.

Synthetic Persona Development:

SRC's ability to develop synthetic personas greatly enhances range exercises and testing, as the personas allow military personnel to utilize realistic, virtual entities for cyber training and testing purposes. These synthetic personas mimic the behaviors and characteristics of potential adversaries, enabling military personnel to practice defending against sophisticated cyber-attacks in a controlled, safe and secure environment. Such training enhances the U.S. Armed Forces' ability to detect, analyze, and respond effectively to cyber threats and strengthens their overall cyber resilience.

Cyber Range Environment Development:

SRC's Cyber Security Evaluation and Testing (CSET) teams provide support by testing and assessing the robustness of military defensive tools employed on networks against cyber threats. By conducting thorough evaluations and threat emulation, SRC CSET teams identify potential weaknesses and recommend solutions to defensive cyber teams. These evaluations help ensure that operations proceed efficiently and timely, allowing defensive teams to reduce the time needed for adjusting tools and troubleshooting issues prior to deployment.

SRC's Cyber Range Support

SRC employs a comprehensive and in-depth approach to cyber range support, encompassing various key elements which are incorporated into cyber range events, documentation, and reporting. Key elements include:

- Cyber range network design, maintenance, and operations
- Cyber range environment design and support
- Adversarial Tactics, Techniques, and Procedures (TTPs)
- Customizable synthetic persona design

These key elements enhance the capabilities of the supported cyber ranges and the U.S. Armed Forces cyber-mission readiness by significantly increasing mission teams' efficiency and reducing down time needed to calibrate tools and troubleshoot potential problems. Below is a more thorough explanation of the key elements**:**

Cyber Range Network Design, Maintenance, and Operations:

SRC's experience in cyber range network design, maintenance, and operations ensures that the supported ranges operate efficiently and securely. SRC has experience in designing and building a cyber range facility and network from the ground up to meet DoD network accreditation requirements and satisfy customer mission needs.

Additionally, SRC's dedicated maintenance and operational support ensures continuous availability and adaptability of the cyber range network, critical for sustained training and testing activities.

Cyber Range Environment Design and Support:

SRC's cyber range environment design, operation, and maintenance enhance the realism and complexity of cyber exercises conducted at the ranges. These realistic cyber environments enable military personnel to practice data-centric cyber defense and response tactics in scenarios that mirror real-world adversarial cyber threats. SRC's expertise ensures that the cyber range environment accurately emulates diverse cyber-attack scenarios, providing invaluable training and learning experiences for the U.S. Armed Forces cyber workforce.

Range Event Documentation and Reporting:

SRC's focus on range event documentation and reporting contributes to the continuous improvement of cyber range exercises. Accurate documentation of the outcomes and responses from cyber exercises allows the U.S. Armed Forces to assess their performance, identify strengths and weaknesses, and refine their cybersecurity strategies. By leveraging insights from range event documentation, cyber defense and response capabilities can be adapted to address emerging threats more effectively.

Adversarial Tactics, Techniques, and Procedures:

SRC's experience in researching and deploying adversarial TTPs enrich the ranges' capabilities. These capabilities enable the creation of sophisticated cyber threats and attacks for realistic cyber range exercises. By simulating diverse adversarial tactics and techniques, the range environments prepare the U.S. Armed Forces to handle advanced and evolving cyber threats effectively, promoting diverse strategies in cyber warfare.

Synthetic Persona Design, Implementation, and Customization:

SRC's synthetic persona design, implementation into cyber range events, and customization add another layer of realism to cyber exercises. Synthetic personas mimic the behaviors of potential adversaries, enabling military personnel to practice cyber defense against realistic threat scenarios. SRC's ability to customize synthetic personas ensures that exercises align with specific training objectives and mission scenarios, enhancing the overall effectiveness of cyber training.

SRC's Contribution to DoD Initiatives

SRC's annual intern program and local high school outreach efforts exemplify its commitment to advancing and expanding the cyber workforce. The intern program focuses on CSET training, cyber analysis, and Open-Source Intelligence (OSINT) training, as well as network engineering, design, and administration training. Interns gain hands-on experience in CSET operations, persona development, range environment design, and range network administration. This comprehensive training is

aligned with the DoD's Cyber Workforce Strategy, providing interns with the skills and knowledge necessary to excel in data-centric cyber operations.

SRC's high school outreach initiative promotes cybersecurity awareness from an early age. By instructing high school students on OSINT practices and the risks of sharing personal information on the internet, SRC contributes to building a cybersecurity-conscious future workforce. This outreach program aligns with the DoD's vision of developing a skilled pipeline of cyber talent from diverse backgrounds.

Conclusion

SRC’s support of cyber and intelligence operations empowers the U.S. Armed Forces to harness data effectively and make more informed decisions, and helps to maintain a competitive edge in modern warfare. Real-time and historical data not only enable informed decision-making but also result in optimized strategies and minimized risks. Enhanced situational awareness, precision targeting, logistics optimization, predictive maintenance, and improved cybersecurity measures further strengthen the armed forces' capabilities and preparedness.

As military and defense operations continue to evolve, the importance of data-centric strategies will grow. SRC's contributions to this approach play a pivotal role in enhancing the U.S. Armed Forces cyber capabilities and overall readiness, ultimately contributing to the success of military missions and national defense. In this era of information-centric warfare, SRC's expertise and commitment to data-centric solutions make them an invaluable partner in strengthening our nation's cybersecurity posture and achieving victory in the cyber domain.