Eric K Corpus

Subject Matter Expert

Summary of Qualifications

A combat veteran and former Cryptologist with over 26+ years of experience in the Intelligence Community and Special Operations. He is a Subject Matter Expert (SME) specializing in the fielding, testing, evaluation, and operational integration of advanced sensitive intelligence, equipment, and technology. Significant experience supporting strategic initiatives including the following: Signals Intelligence (SIGINT); Offensive and Defensive Cyber Operations; Electronic Warfare (EW); Operational Preparation of the Environment (OPE); Counter Terrorism (CT); Hostage Rescue; Counter Proliferation; Sensitive Technical Operations (STO); Alternate Compensatory Control Measures (ACCM)/Special Access Program (SAP) Integration; Information Operations (IO); and Military Deception (MILDEC).

Experience

February 2020 – Present **The Ascendancy Group**

As a Sensitive Activities Advisor responsible for embedded technical and planning solutions in support of sensitive special operations requirements for Naval Special Warfare Units. Performed research and development, integration, and sustainment of SAP/STO, ACCM Programs, and sensitive IO initiatives. Also, supported daily tasking which included Authorities development, CONOP execution, development, and legal review, SIGINT/Cyber/EW integration and capabilities validation, MILDEC, material solutions discovery, Targeting, and Application of Intelligence products. Created planning scenarios for Combatant Command (COCOM) level exercises which have directly informed senior leadership as to the scope and desired end-state as well as ensuring terminal training objectives were achieved. Facilitated information exchanges with external Intelligence Community partners which have laid the groundwork for renewed efforts in support of Great Power Competition (GPC). Provided subject matter expertise in the assessment and evaluation of both Offensive and Defensive Cyber Effects and employment of Expeditionary Cyber Operations capabilities.

December 2019 – February 2020 **SILOTECH Group**

As a Cyber & Non-Kinetic Operations Program Analyst, responsible for providing operations support and technical expertise for Air Combat Command and 16th Air Force staff and subordinate Units. Identified requirements and assisted in the development of training for Airmen assigned to Cyber Mission Force Units. As a member of the Head Quarters Air Combat Command (HQ ACC), A3/2/6KO, Offensive Cyberspace Operations Branch, also advised staff on intelligence and technical issues impacting and capabilities supporting cyberspace, information operations, electronic warfare, and Intelligence, Surveillance and Reconnaissance (ISR) operations.

May 2017 – December 2019 **Navy Cyber Defense Operations Command**

As a Navy Cyber Operations Master Chief and Command Senior Advisor, Directed and managed the strategic direction and daily 24/7 operational employment of 354 Sailors and Civilians for the Navy's only Cybersecurity Service Provider. Defended 3,800 Navy Commands against unauthorized cyber threats.
Responsible for the creation, communication and implementation of standard operating procedures and standardized methodologies and processes. Also, Developed, maintained and published up-to-date security policies, standards and guidelines, and oversaw training and dissemination of security policies and practices. Worked with requirements, budget, acquisition, and installation processes to implement NEXGEN technologies and systems.
Working knowledge of Joint Capabilities Integration Development System (JCIDS) process. Utilized doctrine, organization, training, materiel, leadership and education, personnel, and facilities (DOTMLPF) simulations to identify and provide solution recommendations. Managed a $3.2M operational and training budget, conducted program planning, budget analysis, and executed budget operations that consisted of multiple funding sources and contracts. During this time, ensured command efforts were aligned, including the Project Management Office (PMO) to achieve commander's strategic objectives.

December 2014 – June 2017 **Navy Information Operations Command – Norfolk**

As a Cyber Directorate Senior Advisor and Non-Commissioned Officer In Charge, coordinated and managed the administrative and operational employment of 269 Sailors and Civilians tasked to perform adversary threat emulations, adversarial assessments, and close access objectives by the Navy Red Team, fleet-wide assessments and disseminate cybersecurity best practices by the Navy Blue Team. Executed directed Mission Assurance, Incident Response, and exercise support by 552 Cyber Protection Team. Planned, organized, and met the organization's needs as Knowledge Manager (KM). Developed goals and objectives for organization, conducted specialized research, and standardized tactics, techniques, and procedures (TTPs).

September 2010 – December 2014 **Special Reconnaissance Team Two**

As a Tactical Information Operations (TIO) Operator, forward deployed to austere locations and conducted direct action missions with Naval Special Warfare forces. Tasked to perform precision geo-location, tactical targeting, provide threat warning and force protection utilizing various sensitive technologies and ACCM programs. Conducted specialized and highly sensitive support to Joint Task Force and Joint Force Commanders using Information Operations principles including MILDEC. Provided assessment and technical feedback during the selection of relevant technologies to invest and acquire to support operational requirements. Performed acquisition and contracting of services. Senior Technical Advisor for 310 Officers, SEAL, SWCC, Combat Support and Combat Service Support personnel.

August 2007 – September 2010 **Naval Special Warfare Group Four**

As a Tactical Electronic Warfare Operator, spearheaded and coordinated requirements for manpower, training, and equipping Special Boat Team tactical information operations operators, cryptologic technician augmentees, and highly sensitive cryptologic equipment. Oversaw the development of a requirements generation and capabilities process which identified Joint Threat Warning System Cryptologic Mobile Surface equipment requirements in coordination with Commander, Special Operations Command. Briefed GOFO chaired Special Operations Command Requirements Evaluation Board (SOBRE). Prepared and briefed senior decision makers on NSW generated requirements documents and resourcing impacts to changing requirements to NSW command personnel and subordinate commands. Performed Tactical Electronic Warfare Operations forward deployed onboard Mark V maritime platform and other non-standard craft.

March 2004 – August 2007 **Navy Information Operations Command Kaneohe Bay**

Served as an Airborne Direct Support Electronic Intelligence Supervisor and NATOPS Evaluator. Detected, identified, recorded, and reported data of mission significance inflight. Conducted airborne electronic warfare/reconnaissance/intelligence collections operations which supported objectives for a CNO-sponsored, Multi-Sensor reconnaissance platform executing national and fleet tasking as directed by the Chairman Joint Chiefs of Staff and Theater Commanders.

April 2001 – March 2004 **Joint Intelligence Center Pacific**

As a Cryptologic Support Group (CSG) ELINT Analyst/Watch Supervisor, analyzed operational ELINT data and theatre ballistic missile activity in direct support of Pacific Theater operational forces. Coordinated with Theater and National level ELINT Centers to provide accurate and timely intelligence support. Assisted warfighters with Specific Emitter Identification (SEI), Hull to Emitter (HULTEC) correlation and well as specific country information for Airborne, Surface, and Subsurface Orders of Battle.

April 1998 – April 2001 **Fleet Air and Reconnaissance Squadron TWO**

As an EP-3E Aries II Airborne ELINT Laboratory Operator, conducted in-flight detection, identification, recording, and reporting of data of mission significance. Directly supported airborne EW, Reconnaissance and Intelligence collections operations during multiple SIXTH Fleet Operations and Exercises. Assisted in the development of a new

Squadron High Band Prototype database. Streamlined reporting to external customers and designed a Naval Weapons Fit and Technical Interest List database for the entire EUCOM AOR which proved to be a mission-critical reference guide for all deployed warfighters.

April 1997 – April 1998 **Basic/Technical Training**

Attended Recruit Training Command, Great Lakes, Illinois via the Delayed Entry Program and was meritoriously advanced to E-2. Following Boot Camp, completed Cryptologic Technicians (Technical) "A" School which demonstrated proficiency in the ability to operate and maintain electronic sensors and computer systems, and collect, analyze, exploit, and disseminate Electronic Intelligence (ELINT) all in accordance with fleet and national tasking. Following "A" School, completed Naval Aircrewman Candidate School with additional training at Survival, Evasion, Resistance and Escape School in Brunswick, Maine.

Education and Professional Qualifications

Associate of Arts, (Information Systems), Coastline Community College
University of Virginia Darden School of Business Leadership Course

SANS Cloud Security
GIAC Security Leadership Certification (CSSIP for Managers)
EC Council Certified Ethical Hacker
CompTIA Security+
CompTIA Network+
CompTIA A+
National Security Agency Specialized Training
US SOCOM Senior Enlisted Leadership Course
National Cryptologic Schools EA-279/280
Specialized Survival for Sensitive Reconnaissance Operations Personnel
Survival, Evasion, Resistance and Escape School
Naval Aircrewman Candidate School
Cryptologic Technician Technical "A" School

Security Clearance

TS/SCI with CI Polygraph