

# Jeffrey B. Jordan

✉ [jjordan@ghostedsec.net](mailto:jjordan@ghostedsec.net) | 📞 +1 (206) 580-3599 | 🏠 San Antonio, TX | 🌐 [ghostedsec.net](http://ghostedsec.net)  
📄 [linkedin.com/in/JeffreyBJordan](https://www.linkedin.com/in/JeffreyBJordan)

Top Secret/Sensitive Compartmented Information (TS/SCI) | United States Air Force (Active)

## - Master Résumé -

### Career Summary

- Experienced **Cyber Operations** professional with 13+ years in offensive (OCO) and defensive (DCO) operations, specializing in penetration testing, vulnerability research, digital forensics, and reverse engineering. Proven leader in developing and executing cyberspace strategies, TTPs, and readiness exercises to protect critical infrastructure and ensure mission success. Skilled in training and certifying personnel, analyzing battle damage, and collaborating with interagency and Coalition Forces to achieve national defense objectives. Dedicated to innovation through research, development, and operational testing in high-stakes environments.

### Tech Skills

Linux/Unix • Kali • Windows (user, server) • Networking (Cisco) • Python • Shell Scripting (bash, PowerShell) • VS Code • Git  
• Virtualization (VMware, vSphere, vCenter, ESXi, VirtualBox, Proxmox, Docker)

### Professional Skills

Attention to Detail • Effective Communication • Analytical • Collaborative • Articulate • Problem-Solver • Mentor • Resourceful

### Professional Experience

#### Cyber Warfare Operator

*United States Air Force*

November 2018 – Present

Lackland AFB (JBSA) | San Antonio, TX

#### Advanced Cyber Operations

- **Offensive Operations:** Conducted sophisticated missions for USCYBERCOM, leveraging a \$1.5B national weapons system to disrupt adversary networks, collect intelligence, and execute effects-based operations aligned with Combatant Command objectives. Successfully targeted over 500 enemy systems.
- **Cyber Exploitation & Tools:** Developed and implemented five offensive cyber techniques, enhancing operational capabilities and enabling missions to disrupt critical enemy infrastructure.

#### Training and Leadership

- **Instruction:** Trained and mentored joint force operators in advanced cyber tactics and techniques, preparing teams to utilize \$750M cyber platforms effectively. Played a critical role in the development and revision of Air Force Offensive Cyber Operations courses.
- **Capability Development:** Designed advanced cyber training ranges and created operational scenarios, ensuring readiness and alignment with ACC offensive cyber standards. Conducted 71 mission rehearsals, preparing teams for real-world missions.

#### Innovation and Technical Expertise

- **Tool Development:** Engineered novel solutions for cyber operations, including propagation techniques and custom tools, which expanded operational footholds and supported multi-agency missions.
- **Real-World Application:** Executed counterintelligence, surveillance, and reconnaissance (C-ISR) missions, accessing 20 enemy devices and deploying effects to disrupt adversary command and control (C2) systems. Successfully denied enemy access to months of intelligence by destroying 100GB of critical data during targeted operations.

#### Recognition and Impact

- **Strategic Contributions:** Supported Joint Force Headquarters Cyber (AF)'s top 5 priority targets and helped shape USCYBERCOM's offensive cyber toolkit.
- **Awards:** Recognized with the 67th Cyberspace Wing Meritorious Unit Award for contributions to missions impacting over 2,500 high-priority targets. Consistently lauded by leadership for resilience, innovation, and operational excellence.

### **Defensive Cyberspace Operations**

- **Mission Assurance:** Provided persistent network defense, enabling 24/7 mission assurance for at-home and deployed F-22 operations. Protected critical cyberspace components prioritized by 325 FW senior leadership.
- **Operational Effectiveness:** Utilized active mission defense toolsets to safeguard key terrain and coordinate actions with Air Force and national cyber forces. Successfully analyzed 9 million adversary cyber threats and system alerts, decreasing the enemy attack footprint.
- **Pioneering Achievements:** Played a key role in achieving Initial Operational Capability (IOC) for the first Defensive Cyberspace Operations mission in Air Combat Command (ACC). Established the wing's first cyber planning cell, developed 13 Tactical Techniques and Procedures (TTPs), and earned "best practice" recognition from Headquarters Air Force (HAF/A6).

### **Innovation and Cost-Saving Initiatives**

- **Training Enhancements:** Selected for the Cyber Squadron-Initiative (CS-I) pathfinder program, where I designed a no-cost training lab, saving \$209K. Reengineered network forensic systems, extending data storage capabilities from 90 days to one year, enhancing operational readiness and analysis.
- **Technical Leadership:** Led the installation of four advanced threat detection sensors, positioning the Air Force at the forefront of Cyber Squadron-Initiative (CS-I) capabilities and contributing to the team's recognition with the 2018 ACC General Rawlings Team Award.

### **Recognition and Impact**

- **Awards and Distinctions:** Selected as a Distinguished Graduate in Airman Leadership School (ALS), recognized as a top 10% student leader. Earned multiple accolades, including Airman of the Quarter (2Q16, 1Q17), 9th Air Force Information Dominance/Mission Support Group (MSG) Airman of the Year (2017), and a Secretary of Defense commendation for operational excellence.
- **Strategic Contributions:** Collaborated with Air Combat Command (ACC) and the 35th Intelligence Squadron (IS) to develop cyber response command and control (C2) processes, creating Tactical Techniques and Procedures (TTPs) adopted by 11 Air Force Mission Defense Teams (MDTs) worldwide. Recognized as a Department of Defense (DoD) subject matter expert, featured in mission defense training films used to prepare 45 teams globally for cyber readiness.

### **System Maintenance and Repair**

- **Comprehensive Inspections:** Inspected, repaired, and installed fixed/mobile radio systems supporting over 6,800 personnel across AFNORTH and the 325th Fighter Wing, ensuring mission readiness.
- **Preventive Maintenance:** Conducted preventive maintenance and inspections on 33 towers and 4 control stations for the Installation Warning System (IWS), guaranteeing uninterrupted alert capabilities.
- **Critical Repairs:** Identified and replaced faulty components in high-frequency radios and power supplies, restoring homeland security and air control communication links vital to training and operations.

### **Mission Assurance**

- **F-22 Mission Support:** Maintained and repaired ground-to-air communication links, enabling seamless operations for the USAF's only F-22 pilot training mission and Air Battle Manager School.
- **PA System Operations:** Operated and maintained Public Address (PA) systems, providing technical support and training to base customers for event execution and mission-critical announcements.
- **Deployed Operations:** Repaired and optimized communication systems during deployment, sustaining \$28M in C4 assets and supporting multinational efforts with 9 partner nations.

### **Operational Upgrades and Cost Savings**

- **In-House Solutions:** Devised in-house fixes for damaged equipment, including re-soldering faulty power cables and refurbishing tactical radios, saving over \$27,000 in repair costs and reducing delays.
- **System Upgrades:** Led a \$1.1M communication system upgrade, completing the project four months ahead of schedule and delivering enhanced operational capabilities.
- **Cost Avoidance:** Pinpointed damaged RF filter modules and cables in critical systems, repairing them in-house to avert downtime and saving over \$10K in parts costs.

## Event and Mission Support

- **High-Profile Events:** Delivered flawless communication setups for events like the Gulf Coast Salute and Florida Governor's quarterly meeting, earning commendations from senior leadership.
- **Seamless Event Execution:** Set up and operated sound systems for critical events, including the 325 MSG change of command and large-scale exercises involving 55,000 guests, projecting a professional Air Force image.
- **Global Support:** Organized communication networks for 58 World Phones, enabling operational success in 5 nations and supporting 18 high-priority missions.

## Inventory Management and Training

- **Equipment Accountability:** Trained replacement personnel and managed inventories for \$800K in high-value assets during deployments, ensuring mission continuity.
- **Asset Oversight:** Managed \$495K in communication assets, issuing 225 devices and maintaining 100% accountability for operational readiness.
- **Readiness Restorations:** Conducted inventory audits and restored operational functionality for 78 Blue Force Trackers, safeguarding \$240K in mission-critical assets.

## Recognition

- **Award-Winning Performance:** Garnered multiple accolades, including Airman of the Month and Quarter, for exceptional technical expertise and dedication to mission success in a deployed environment.
- **Leadership Appreciation:** Received letters of appreciation and recognition from senior leadership for significant contributions to events and mission assurance.
- **Strive for Excellence:** Deployed to the Horn of Africa to maintain \$28M in communication assets supporting 33 missions; earned multiple awards, including Distinguished Graduate in technical training and Airman of the Year.

## Education & Training

---

### Bachelor of Science (B.S.) Computer Networks & Cybersecurity (IN PROGRESS) \*(94% Complete | 113/120 credits)

- University of Maryland Global College (UMGC)
  - Honor Societies (Alpha Sigma Lambda (ΑΣΛ) | Phi Kappa Phi (ΦΚΦ) | Upsilon Pi Epsilon (ΥΠΕ))
  - UMGC Cyber Team

### Computer Network Operations Qualification Course (CNOQC) July 2020

- National Cryptologic University (NCU) – (CYBR3422)

### Associate in applied science (A.S.): Cybersecurity July 2019

- Community College of the Air Force (CCAF)

### Associate in applied science (A.S.): Electronic Systems Technology December 2013

- Community College of the Air Force (CCAF)

### Associate in arts (A.A.): General Studies May 2010

- North Florida Community College (NFCC) – Magna Cum Laude (3.71 GPA)
  - Honor Society (Phi Theta Kappa (ΦΘΚ))
  - Brain Bowl Competitor / Team Leader

## Training

### National Cryptologic University (NCU)

- (NCU) Purple Team Tactics – Breach Prevention & Detection (CYBR369) August 2023
- (NCU) Advanced Penetration Testing, Exploit Writing, & Ethical Hacking (CYBR3660) July 2023
- (NCU) Defeating Advanced Adversaries – Implementing Kill Chain Defenses (CYBR2599) June 2023
- (NCU) Forensics, Incident Response, & Threat Hunting (CYBR2508) June 2023
- (NCU) Red Team Operations & Adversary Emulations (CYBR2565) June 2023
- (NCU) Metasploit Kung Fu for Enterprise Pen Testing (CYBR2580) June 2023
- (NCU) Web App Penetration Testing & Ethical Hacking (CYBR2542) May 2023
- (NCU) Network Penetration & Ethical Hacking (CYBR2560) April 2023
- (NCU) Ultimate Hacking Expert Level (CYBR2102) July 2022
- (39<sup>th</sup> IOS, Air Force) Classroom Instructor Course (CIC) July 2021
- (390<sup>th</sup> COS, Air Force) Operator Mission Qualification Training (MQT) August 2020
- (Root9B) Applied Cyber Operations Training (ACOT) May 2019

- (39<sup>th</sup> IOS, Air Force) Cyber Warfare Operations (CWO) Course
- (ROOT9B) Network Characterization Course

March 2019  
August 2016

## Professional Certifications

---

**CompTIA:** Cloud+, CySA+, PenTest+, Linux+, Security+, Network+, A+

### Cybersecurity

- CompTIA Secure Infrastructure Specialist (CSIS)
- CompTIA Network Vulnerability Assessment Professional (CNVP)
- CompTIA Network Security Professional (CNSP)
- CompTIA Security Analytics Professional (CSAP)
- CompTIA Secure Cloud Professional (CSCP)

### Infrastructure

- CompTIA IT Operations Specialist (CIOS)
- CompTIA Linux Network Professional (CLNP)
- CompTIA Systems Support Specialist (CSSS)
- CompTIA Cloud Admin Professional (CCAP)

### (ISC)<sup>2</sup>:

- Certified in Cybersecurity (CC)
- Certified Information Systems Security Professional (CISSP)

### SANS/GIAC:

- GIAC Certified Forensic Analyst (GCFA)
- GIAC Certified Incident Handler (GCIH)
- GIAC Advisory Board Member

**Cisco:** CyberOps Associate (CCNA CyberOps)

### DoDD 8140/8570:

- Information Assurance Technical (IAT) Level III
- Information Assurance Management (IAM) Level III
- Information Assurance System Architecture and Engineering (IASAE) Level II