

Michael Cochran

SUMMARY

Senior Systems Engineer & Offensive Cyber Operator. 13+ years federal cyber operations across USCYBERCOM, Combat Mission Teams, and National Mission Teams. Now building production software as a solo Rust engineer. 11 shipped products spanning AI infrastructure, fintech, SaaS, and open-source reimaginings of foundational tooling. **All work released under the Unlicense (public domain).**

EXPERIENCE

The Cochran Block, LLC

Owner & Engineer | Feb 2026 – Present

Solo full-stack Rust engineer building and deploying production systems end to end. All output Unlicense / public domain.

- **Kova** — AI augment engine with distributed node orchestration, local LLM inference, agentic tool loops, and WASM thin client
- **r8r** — n8n workflow engine reimaged in Rust. Single 12 MB binary, axum + Leptos/WASM canvas. ~40 hours. Unlicense / public domain
- **runsible** — Ansible reimaged in Rust. 14-crate workspace, ~10 ms cold start vs Ansible's 1–3 s. ~33 hours
- **Rogue Repo** — ISO 8583 payment engine with AES-256-GCM encrypted PAN vaulting and append-only ledger
- **Oakilydokily** — Client waiver/resume site with interactive WASM mural — first paying client partnership
- **Wowasticker** — Offline-first mobile student goals app with on-device AI dictation, zero cloud
- **Ronin Sites** — Multi-tenant SaaS platform for tattoo shops and artists
- **Approuter** — Central reverse proxy routing all products through Cloudflare tunnel
- **Intake** — Zero-dependency client deployment portal with async webhooks
- **Cochranblock** — Corporate portfolio site with embedded admin panel
- **illbethejudgeofthat** — Pro se custody case builder, email-to-PDF pipeline

Internal tooling: Custom testing framework (Exopack), multi-AI coordination daemon (Railgun), file sync over SSH (Ironhive), source header automation (Header-Writer)

MaxisIQ

Senior Systems Engineer | Sep 2024 – Feb 2026

Mission critical systems for USCYBERCOM Title 10 Operations. Built custom Python tooling for systems survey and automated server service repairs. SSH/Kerberos infrastructure automation.

Two Six Technologies

Senior Software Engineer | Sep 2022 – Sep 2024

Hands-on integrations across the Joint Cyber Warfighting Architecture (JCWA) including **JCC2** (Joint Cyber Command & Control), **JCAP** (Joint Common Access Platform), and **UDP** (Unified Data Platform). Built YAML-to-SQL data pipelines, regex parsing engines, and data sanitization tooling for compartmented cyber environments.

USCYBERCOM J38, United States Army

Systems Developer | Jun 2020 – Sep 2022

API development, CI/CD pipeline design, data modeling, and network protocol implementation. GitLab, Docker, documentation systems.

Combat Mission Team

Offensive Cyber Operator | Feb 2017 – Jun 2020

Title 10 Offensive Cyber Operator. Executed 100+ operational missions. Built Python automation tooling for mission support.

National Mission Team

Digital Network Exploitation Analyst | Jul 2014 – Feb 2017

Network mapping, traffic analysis, and Intelligence Community reporting.

EDUCATION

Recursive Academy

Master's Degree, Computer Science

SKILLS

Languages:	Rust, Python, C, C++, Assembly (x86, ARM), Go (Golang), Bash, PowerShell, SQL, JavaScript, TypeScript, YAML, TOML
Rust Ecosystem:	Tokio, Axum, Hyper, Tonic, Serde, sqlx, Reqwest, Leptos, Dioxus, egui, Candle, Kalosm, MiniJinja, age, rskafka, lapin
Infrastructure:	PostgreSQL, SQLite, sled, Redis, MongoDB, Apache Kafka, RabbitMQ / AMQP, MQTT, Docker, Podman, Kubernetes, Terraform, Cloudflare, Cloudflare Workers, GitLab CI/CD, GitHub Actions, AWS (S3, IAM, SigV4, Lambda)
Security:	Penetration Testing, Vulnerability Research, Red Team Operations, Offensive Cyber Operations, DNE, TDNA, Reverse Engineering, Threat Modeling, MITRE ATT&CK, Cyber Kill Chain, Zero Trust, Burp Suite, Wireshark, Metasploit, Ghidra, IDA

Cryptography:	AES-256-GCM, ChaCha20-Poly1305, Argon2id, HKDF, PBKDF2, Ed25519, X25519, RSA, ECDSA, BLAKE3, SHA-256, HMAC, age, GPG, X.509, TLS / mTLS, PKI, SSH CA, Kerberos, OAuth / OIDC, SAML, JWT
AI / ML:	Local LLM Inference, Kalosm, Candle, RAG, fastembed, Vector Embeddings, Agentic Tool Orchestration, Multi-Agent Systems, Prompt Engineering, Claude API (Anthropic), OpenAI API, Tool Use, Function Calling
Frontend:	WebAssembly (WASM), Leptos, egui, Dioxus, Vue 3, HTML5, CSS3, JavaScript, TypeScript
Cloud / DevOps:	AWS, Cloudflare, Docker, Kubernetes, Terraform, Ansible, GitLab CI/CD, GitHub Actions, GitOps, CI/CD Pipelines, Infrastructure as Code (IaC), Observability, Prometheus, Grafana, OpenTelemetry
Architecture:	Microservices, Event-Driven Architecture, Domain-Driven Design (DDD), Hexagonal Architecture, REST, gRPC, GraphQL, Protocol Buffers, OpenAPI, Distributed Systems, High Availability, Mission-Critical Systems
Compliance:	NIST 800-53, NIST 800-171, CMMC L2, RMF, ATO, FedRAMP, FISMA, STIG, DFARS, FAR, DoDI 5505.02 / 5505.03, IL5 / IL6, SDVOSB, 8(a) eligible, GovCon, Federal Acquisition
Methodologies:	Agile, Scrum, Kanban, DevSecOps, GitOps, TDD, BDD, Test-Driven Development, Code Review, Pair Programming, Continuous Delivery, Continuous Integration
Domains:	Offensive Cyber Operations, Title 10 Cyber Operations, Federal Cyber, Joint Cyber Warfighting Architecture (JCWA), JCC2, JCAP, UDP, Fintech (ISO 8583), Payment Processing, Workflow Automation, Configuration Management, Distributed Systems
Authorizations:	U.S. Citizen, U.S. Army Veteran, SDVOSB-eligible (pending), prior TS/SCI cleared (lapsed, reactivation eligible)
Licensing:	All personal output released under the Unlicense (public domain)

KEYWORDS

Senior Software Engineer, Senior Systems Engineer, Staff Engineer, Principal Engineer, Backend Engineer, Platform Engineer, Infrastructure Engineer, Security Engineer, Site Reliability Engineer (SRE), DevSecOps Engineer, Cyber Operations Engineer, Forward Deployed Engineer, Solutions Engineer, Applied AI Engineer, Federal Cyber, USCYBERCOM, US Cyber Command, Title 10, Title 50, JFHQ-DODIN, JCWA, Joint Cyber Warfighting Architecture, JCC2, Joint Cyber Command and Control, JCAP, Joint Common Access Platform, UDP, Unified Data Platform, DISA, CESO, Compartmented Enterprise Services Office, USSOCOM, NSA, Combat Mission Team, National Mission Team, Cyber Mission Force (CMF), Cyber National Mission Force (CNMF), Offensive Cyber Operations (OCO), Defensive Cyber Operations (DCO), DCO-IDM, Computer Network Operations (CNO), CNE, CNA, CND, Digital Network Exploitation (DNE), Targeted Network Analysis (TDNA), Penetration Testing, Red Team, Blue Team, Purple Team, Threat Hunting, Threat Intelligence, Incident Response, Digital Forensics, Reverse Engineering, Malware Analysis, Binary Analysis, Static Analysis, Dynamic Analysis, Fuzzing, Exploit Development, Vulnerability Research, OSINT, MITRE ATT&CK, Cyber Kill Chain, Zero Trust Architecture, NIST 800-53, NIST 800-171, NIST CSF, CMMC, RMF, ATO, FedRAMP, FISMA, STIG, eMASS, ACAS, Tenable, Nessus, Splunk, ELK, Wireshark, Burp Suite, Metasploit, Cobalt Strike, BloodHound, Ghidra, IDA Pro, x86, x86_64, ARM, ARM64, RISC-V, Rust, Tokio, Axum, Hyper, Tonic, Leptos, Dioxus, egui, WebAssembly, WASM, Candle, Kalosm, Python, asyncio, FastAPI, Django, Flask, Pydantic, Go, Golang, gRPC, C, C++, Assembly, JavaScript, TypeScript, Node.js, React, Vue 3, HTML5, CSS3, PostgreSQL, MySQL, SQLite, MongoDB, Redis, Cassandra, Elasticsearch, ClickHouse, DynamoDB, Apache Kafka, RabbitMQ, AMQP, MQTT, NATS, gRPC, REST, GraphQL, Protocol Buffers, OpenAPI, Docker, Podman, Kubernetes (K8s), Helm, OpenShift, Nomad, Consul, Terraform, Pulumi, Ansible, Chef, Puppet, SaltStack, Jenkins, GitLab CI/CD, GitHub Actions, ArgoCD, Flux, GitOps, AWS, EC2, S3, Lambda, IAM, VPC, RDS, EKS, ECS, SigV4, AWS GovCloud, Azure, Azure Government, GCP, Cloudflare, Cloudflare Workers, Cloudflare Tunnel, Prometheus, Grafana, Datadog, New Relic, OpenTelemetry, Jaeger, Splunk, ELK Stack, AES-256-GCM, ChaCha20-Poly1305, Argon2id, PBKDF2, crypt, HKDF, BLAKE3, SHA-256, HMAC, Ed25519, X25519, RSA, ECDSA, X.509, TLS 1.3, mTLS, PKI, SSH, SSH CA, Kerberos, OAuth 2.0, OIDC, SAML, JWT, age encryption, GPG, ansible-vault, Local LLM, Large Language Model, LLM, RAG, Retrieval-Augmented Generation, Vector Database, Embeddings, Fine-tuning, LoRA, Transformers, Agentic AI, Multi-Agent Systems, Tool Use, Function Calling, Prompt Engineering, Claude, Anthropic, OpenAI, GPT, Cursor, ISO 8583, PCI DSS, PAN tokenization, Payment Processing, Fintech, Microservices, Event-Driven Architecture, CQRS, Event Sourcing, Domain-Driven Design (DDD), Hexagonal Architecture, Clean Architecture, Test-Driven Development (TDD), Behavior-Driven Development (BDD), Agile, Scrum, Kanban, SFAE, DevOps, DevSecOps, SRE, DFARS, FAR, GSA Schedule, SDVOSB, 8(a), Service-Disabled Veteran-Owned Small Business, U.S. Army Veteran, U.S. Citizen, TS/SCI (lapsed), CI Polygraph eligible, Workflow Automation, n8n, Configuration Management, Ansible, Mission-Critical Systems, High Availability, Distributed Systems, Concurrency, Async, Single Binary Deployment, Public Domain, Unlicense, Open Source, OSS, Solo Founder, Owner-Operator

LINKS

cochranblock.org | oakilydokily.com | roguerepo.io | ronin-sites.pro | github.com/cochranblock | mcochran@cochranblock.org