William Chuang

Tucson, AZ
williamhschuang@gmail.com williamchuang.github.io

Summary of Qualifications

- **Strategic Thinker (INTJ)**: Focused on long-term, high-impact solutions in AI-driven cryptanalysis, OSINT, and cybersecurity.
- **Advanced Math & Physics:** Deep expertise in hyperbolic geometry, Kleinian groups, Galois theory, crucial for secure algorithm design.
- **Robust R&D:** 10+ years at respected institutions (Arizona, SFSU, Penn State, NTU), applying theoretical methods to practical challenges.
- **Security & Cryptography:** Applied curvature, limit sets, and Galois groups in post-quantum encryption and secure data protocols.
- **OSINT & Cybersecurity Research:** Self-studying Open-Source Intelligence (OSINT), pentesting, network forensics, and adversarial ML applications in threat detection.
- **Machine Learning & Data Security:** Applying ML models to system log analysis, TCP/IP traffic inspection, firmware integrity verification, and network anomaly detection.
- **Computational Proficiency:** Python (NumPy, scikit-learn, PyTorch), R, C/C++, Java, Lisp, Mathematica, Linux/Bash scripting, and reverse-engineering low-level firmware; built large-scale cryptography tools.

Education

University of Arizona (Expected Spring 2025)
M.S. in Mathematics, advanced Ph.D.-level coursework

San Francisco State University (Spring 2022)
M.A. in Mathematics; Thesis on Schottky groups (Advisor: Dr. C.-K. Lai)

University of San Francisco (Fall 2018)
B.S. in Mathematics, Minor in Computer Science, GPA: 3.88/4.00, Honors

Core Competencies

Mathematical Cryptography & Security:
Hyperbolic geometry, Kleinian groups, post-quantum cryptography, topological vulnerabilities.

Developing a novel encryption framework leveraging group actions on neural networks rather than solutions of differential equations. This approach, independently conceived and later found to parallel the motivation behind Poincaré's Fuchsian groups and monodromy, restructures security landscapes in the post-quantum era by embedding cryptographic transformations within geometric symmetries.

Data Analysis & Machine Learning:
Transformer architectures (multi-head attention), autoencoders, geometric/topological ML approaches.

Algorithm & HPC Development:
Python/C++ for large-scale data, GPU-accelerated ML, system-level optimization.

Research & Technical Writing:
Multiple publications/presentations; formal proof tools (Lean 4, LLMs).

AI-Augmented Intelligence Analysis & OSINT Automation:
Developing transformer-based (local LLM) AI agents trained on intelligence cycle methodologies (e.g., Heuer's structured analysis, HUMINT techniques) for real-time data fusion, deception detection, and adversarial influence modeling.

Human Factor Security & OSINT:
Defending against psychological manipulation, decoding body language, behavioral profiling, lie detection via baseline analysis, NLP for communication security, countering mind control tactics, and influence operations in intelligence settings.

Cognitive & Influence Security:
Adversarial intelligence analysis, AI-enhanced OSINT gathering, NLP-driven deception detection, psychological profiling via transformer models, and social engineering countermeasures.

Relevant Research Experience

University of Arizona (2022–Present)
- *Prof. S. Sethuraman:* Real analysis; self-studied stochastic processes for cryptanalysis.

- *Prof. S. Cherkis:* Explored Nahm equations, geometric field theories, and used Lean 4+LLMs for secure AI.
- *Prof. N. Hao:* RTG Project on transformer attention scaling.
- *Prof. C. Haessig:* Investigated corresponding polynomials of Galois gorups by writing Python code, self-studying this for cryptographic classification.
- *Prof. D. Glickenstein:* Mentored a project reconstructing Mirzakhani's study on hyperbolic geometry and closed geodesics, with self-study on its application for encryption using transformer architectures and autoencoders.

San Francisco State University (2019–2022)
- Computed Hausdorff dimension of Schottky groups; applied fractal geometry for data obfuscation.
- Applied the prime geodesic theorem to secure high-dimensional data.

Pennsylvania State University (2017–2018)
- Investigated Hardy's proof of uniform distribution (pseudo-random generation).
- Studied topological invariants for encryption algorithms.

NTU—LeCosPA (Pre-Baccalaureate, 2011–2013)
- Researched TQFT, AdS/CFT, and vacuum energy; early work in quantum information.

Additional Research Projects

Self-Study: Semisimple Rings and Radicals in Coding Theory and Cryptography
Based on Prof. Klaus M Lux's lecture (Spring 2025), this project explores the role of semisimple rings and the Jacobson radical in coding theory and cryptography. Topics include linear codes over rings (e.g., $\mathbb{Z}_4$), group algebras, ring-based cryptosystems (NTRU, Ring-LWE), and ten concrete examples illustrating how nontrivial radicals influence cryptographic security.

Self-Study: AI-Driven Network & Firmware Security Analysis
Applying machine learning to detect anomalies in system logs, TCP/IP traffic, and firmware integrity. Researching adversarial ML techniques for cyber threat detection, focusing on vulnerabilities in processors (e.g., AMT), chipsets, embedded firmware, and network traffic patterns. Investigating anomaly detection across all OSI layers and forensic-level system monitoring.

- **Vendor-Specific Commands (VSCs) in ESP32 ROM:**
  Recent research (Tarlogic Security) has uncovered hidden VSCs in the publicly available ESP32 ROM, enabling attackers to execute undocumented firmware functions. Given that over 1 billion Bluetooth and IoT devices use ESP32-based microcontrollers, adversaries can exploit these VSCs for:
  - **Unauthorized access, remote execution, and persistence mechanisms** in IoT networks.
  - **Covert control over ESP32-adjacent IoT devices** through Bluetooth Low Energy (BLE) and WiFi communication.
  - **Firmware-level exploits** that compromise security-sensitive environments.
  - **Impersonation attacks & permanent infections:** Exploitation of this backdoor allows hostile actors to **conduct identity spoofing, covert data injection, and long-term persistence in mobile phones, computers, smart locks, and medical equipment**. By bypassing standard code audit controls, adversaries can embed malware at the firmware level, rendering traditional security mechanisms ineffective.
- **TCP/IP Anomaly Detection and Network Traffic Patterns:**
  Applying AI-driven network forensics to identify and classify deviations in TCP/IP traffic, with a focus on:
  - **Passive traffic analysis** to detect anomalous packet headers, timing irregularities, and encrypted payload injection.
  - **Signature-based detection** for identifying known malware patterns in packet structures.
  - **Behavioral anomaly detection** using transformer-based AI models to track deviations in baseline network behavior.
- **Forensic OSI-Layer Monitoring:**
  Investigating AI-enhanced intrusion detection across all OSI layers, including:
  - **Layer 2 (Data Link)**: Identifying MAC spoofing, ARP poisoning, and rogue device injection.
  - **Layer 3 (Network)**: Analyzing suspicious ICMP tunneling and unauthorized VPN encapsulation.
  - **Layer 4 (Transport)**: Detecting anomalous TCP/UDP flow patterns in botnet or DDoS attack scenarios.
  - **Layer 7 (Application)**: Monitoring HTTP, DNS, and MQTT-based IoT command-and-control (C2) communications.
- **Reverse Engineering & AI-Assisted Intrusion Detection:**
  - Disassembling firmware to uncover hidden commands, privilege escalation pathways, and unauthorized access points.
  - **Developing transformer-based AI anomaly detection** to monitor firmware execution and detect irregular command sequences.
  - **Applying differential firmware analysis** to compare modified vs. original versions, detecting unauthorized alterations.
- **Supply Chain & OT/IoT Security:** Assessing the impact of compromised firmware in supply chain

attacks and **developing AI-driven intrusion detection for embedded systems**.
- **Developing Countermeasures:**
  - Firmware hardening strategies to prevent **unauthorized command execution** in microcontrollers.
  - **Runtime monitoring for AI-enhanced anomaly detection** in embedded devices.
  - OSINT-driven threat intelligence tracking **to detect active exploitation campaigns**.

Potential Applications:
- **Securing IoT/OT devices against firmware-based backdoors and supply chain risks.**
- **Enhancing AI-driven intrusion detection (IDS) for network-connected embedded systems.**
- **Developing forensic methods for detecting unauthorized access via Intel AMT/VSC exploits.**
- **Applying SIGINT/Spectrum Analysis to detect covert device exfiltration via unauthorized RF transmissions.**
- **Hardening medical and critical infrastructure devices against firmware-based impersonation attacks.**

Self-Study: RF Signal Analysis for SIGINT & Cybersecurity
Applying spectrum analysis, software-defined radio (SDR), and machine learning to detect, classify, and mitigate anomalous RF signals, including the detection of unauthorized cellular simulators (such as IMSI catchers, rogue base stations, and spoofed cell towers used by malicious actors for surveillance, data injection, or signal jamming). Researching RF propagation, modulation techniques, and counter-SIGINT strategies.

Self-Study: AI-Driven Cognitive Security & OSINT Defense
Designing AI-powered analyst teams using transformers (local LLMs) for autonomous intelligence gathering, behavioral profiling, and deception detection. Researching automated influence analysis and adversarial social engineering defense using Heuer's methods (Analysis of Competing Hypotheses, Structured Analytical Techniques).

Self-Study: AI-Driven Narrative Simulation & Influence Modeling
Researching AI-driven frameworks for strategic narrative generation, adversarial influence simulations, and predictive modeling of geopolitical discourse. Developing transformer-based AI for policy impact analysis, disinformation detection, and automated strategic communications. Exploring AI-enhanced wargaming environments to test leadership messaging strategies, adversarial competition, and cognitive warfare principles. Studying structured analytic techniques (SATs), psychological operations (PsyOps), and counter-deception models to advance information dominance in government, defense, and corporate intelligence applications.

Self-Study: Emerging Sensing Technologies & Counter-Surveillance
Self-studied laser-based Non-Line-of-Sight (NLoS) imaging capable of reconstructing rooms through keyholes or occlusions. Currently researching counter-surveillance techniques using hyperbolic transformers to detect or interfere with adversarial NLoS imaging. Exploring future applications to human-computer interaction (HCI) via remote gesture sensing through walls and barriers. Emphasizing dual-use applications for both intelligence collection (next-generation surveillance) and defensive countermeasures (anti-surveillance and physical security augmentation).

Self-Study: Multimodal Environmental Sensing — RF, Ultrasound, & IoT Fusion for Privacy, Healthcare, HCI, & Real-Time Polygraph Workflows
Researching multimodal environmental sensing combining WiFi-based human pose estimation (RF DensePose), supersonic/ultrasound sensing using smartphone and IoT device speakers/microphones, and cooperative swarm sensing across distributed devices. Applying hyperbolic transformers for both sensing enhancement and privacy-preserving countermeasures.
This study spans:
- **Privacy-Preserving Counter-Surveillance**: Developing adversarial signal injection and hyperbolic signal shaping techniques to defend against unauthorized through-wall or through-device imaging by adversarial actors.
- **Home Healthcare & Elderly Monitoring**: Real-time non-contact monitoring using WiFi signals, ultrasound echoes from smartphones/IoT speakers, and fusion across environmental sensors to detect posture, falls, and respiratory patterns.
- **First Responder & Disaster Recovery**: Using RF + ultrasound hybrid sensing for detecting human presence through smoke, debris, or walls in collapsed buildings or emergency rescue operations.
- **Global Anatomical Data for AI Surgical Training**: Passive collection of anonymized human motion and anatomical movement data across populations using everyday devices, building a global real-time anatomical dataset to train AI surgeons and autonomous medical robots.
- **Human-Computer Interaction (HCI) & Real-Time Polygraph Workflows**: Developing gesture/movement-based control interfaces using combined RF, ultrasound, and environmental sensing—enabling seamless, touchless interaction across AR/VR workspaces, smart homes, autonomous vehicles, and advanced research environments where polygraph testing and biometric sensing require non-invasive monitoring of physiological responses.
- **Neuromodulation via Ultrasound for Cognitive & Hypnotic Studies**: Investigating how *low-intensity focused ultrasound (LIFU)* and *transcranial ultrasound stimulation (TUS)* can influence *cognitive states, suggestibility thresholds, and stress resilience.* Exploring *behavioral entrainment, subconscious priming, and cognitive modulation* using controlled *ultrasound-based hypnotic induction* techniques.

This integrates:

- **Wireless Physical Layer Security** (RF/ultrasound channel obfuscation)
- **Hyperbolic Geometry for Signal Processing**
- **AI-Driven Multimodal Sensor Fusion**
- **Medical Imaging via Passive Sensing**
- **Edge AI on Smartphones, IoT, and Wearables**
- **Cognitive Ergonomics for Real-Time Polygraph HCI**
- **AI-Augmented Neuromodulation for Behavioral & Cognitive Influence**

Applications span:

- Privacy-preserving smart home environments (smartphones doubling as silent guardians).
- Telemedicine with non-contact remote diagnostics.
- First responder deployment in smart disaster zones.
- HCI innovations for polygraph-integrated security screenings, behavioral analytics, and biometric monitoring.
- Spatial computing interfaces for intelligence analysis, multi-modal sensemaking, and collaborative situational awareness.
- Ultrasound-based **hypnosis research** for cognitive priming, stress modulation, and suggestibility analysis.
- AI-enhanced cognitive neuroscience research into **non-invasive behavioral conditioning techniques**.

Self-Study: Transformer-Based Analysis & Countermeasures for EM/Stealth Radiation Document Espionage

Investigating advanced espionage techniques where adversarial actors deploy combined radiation and electromagnetic (EM) waves—ranging from terahertz and zeta waves to backscatter and passive reflectometry—to covertly scan printed documents on desks, bookshelves, or in file cabinets, retrieving content without physical access.

This research integrates:

- Applying transformer-based AI to reconstruct potential document exposures by reverse-engineering scanned data footprints.
- Developing hyperbolic transformer architectures to detect signal anomalies, leveraging curvature-sensitive embeddings to highlight unnatural EM reflections characteristic of covert scanning.
- Applying SDR (Software-Defined Radio) and real-time spectrum analyzers to continuously monitor the local EM environment, detecting covert scanning transmissions in real time.
- Exploring adversarial radiative shielding using AI-optimized metamaterials, structured electromagnetic interference (EMI), and dynamic scattering techniques to actively distort or mask document content.
- Formulating inverse problems to infer adversarial scanner configurations from detected emission patterns, enabling real-time counterintelligence alerts for classified or proprietary document protection.
- Integrating findings into comprehensive counter-surveillance and physical security intelligence (PHYSINT) toolkits, linking document-level monitoring with broader facility security intelligence.

Potential Applications:

- Protection of classified documents, trade secrets, and sensitive archives in government, defense, and corporate environments.
- Continuous EM environment monitoring for SCIFs, executive boardrooms, and high-risk offices.
- Design of next-generation secure office spaces, blending AI-guided shielding, active jamming, and smart concealment within physical spaces.

This project advances Prodeo's future capabilities in AI-enhanced counterintelligence, blending SIGINT, PHYSINT, and adversarial ML into adaptive counter-surveillance systems.

Self-Study: Advanced Defense Systems — Next-Generation Projectiles & Subsurface Security

Researching emerging methods for precision-guided projectiles, terrain-penetrating munitions, and hybrid-domain deterrence systems. Focus includes:

- Physics and engineering of projectile-launch mechanisms leveraging electromagnetic, plasma-assisted, and hybrid propulsion technologies.
- Subsurface security challenges including adversarial tunneling, underground domain awareness, and sensor fusion.
- AI-enhanced modeling for optimizing projectile trajectories across air, water, and solid earth.
- Integration of under-terrain sensing, autonomous subterranean drones, and real-time countermeasures within broader C4ISR ecosystems.
- Cross-domain fusion of subsurface, underwater, and near-space kinetic capabilities for next-generation integrated deterrence.

Potential Applications:

- Strategic infrastructure protection (nuclear silos, undersea cables, communication hubs)
- Defense against adversarial tunneling, mining, and subsurface infiltration
- Rapid-response countermeasure systems for critical asset protection
- Next-generation coastal and inland defense blending subsurface, surface, and aerial ISR

Note: This self-study also supports future consulting capabilities under Prodeo, offering dual-use solutions for defense clients, critical infrastructure operators, and advanced engineering teams exploring subsurface and hybrid-domain challenges.

Self-Study: Counter-Detection for Terrain-Penetrating Munitions Using Gravitational Waves &

Neutrino Imaging
Researching advanced sensor and detection systems leveraging gravitational waves and neutrino-based sensing to detect and map terrain-penetrating munitions and subsurface threats. This approach addresses current limitations in radar, seismic, and acoustic detection by:

- Exploring gravitational perturbations caused by projectile movement or underground excavation, detectable via space-based or ground-based gravitational wave sensors.
- Investigating neutrino backscattering or diffraction signatures from dense subterranean objects (e.g., munitions, tunnels, or reinforced structures).
- Applying hyperbolic transformer-based AI to fuse multi-physics sensor data into coherent, real-time subsurface threat models.
- Developing anomaly detection techniques for long-duration monitoring, highlighting subtle gravitational or neutrino signal deviations against natural background noise.
- Studying feasibility of distributed sensor networks (space-ground hybrid) for persistent monitoring of critical subsurface assets, infrastructure, and border regions.

Potential Applications:

- Early warning and tracking of deep-penetration munitions and adversarial excavation efforts.
- Dual-use scientific sensors for both astrophysical research and applied national security.
- Real-time subsurface "neutrino radar" for next-generation underground domain awareness.

Note: This study supports Prodeo's future capabilities in dual-use subsurface ISR and gravitational/neutrino-based intelligence applications, relevant to both defense clients and scientific partners.

Self-Study: Directional Antennas and RF-Based Counter-Surveillance
Investigating RF signal propagation, surveillance countermeasures, and the use of directional antennas (e.g., Arrow II Yagi) with handheld radios and software-defined radio (SDR) for security operations and technical sweeps.

- **RF Bug Sweeps and Surveillance Detection:**
  - Applied mobile directional antennas to detect, localize, and characterize unauthorized RF emissions in secure environments.
  - Performed spectrum analysis using SDR to identify anomalies across VHF/UHF/microwave bands — including hidden transmitters, backscatter devices, and wireless bugs.
  - Analyzed signal strength gradients, Doppler shifts, and side-lobe reflections to triangulate covert emitters.
- **TSCM (Technical Surveillance Countermeasures) Applications:**
  - Studied use cases of portable antenna arrays for bug sweeps, RF shielding verification, and wireless intrusion audits.
  - Researched directional signal hunting, covert channel mapping, and adversarial RF signature spoofing.
  - Integrated open-source SDR tools (e.g., GQRX, SDR++) with real-time visualization for detecting surveillance infrastructure.
- **Operational Field Considerations:**
  - Evaluated deployment scenarios for mobile TSCM operations in executive offices, SCIFs, and mobile command vehicles.
  - Explored RF forensics for identifying digital eavesdropping attempts and side-channel leakage.

Self-Study: Physical Infrastructure Security via Plumbing and Sewer Systems
Explored the risks and countermeasures associated with adversarial access to facilities through altered or rerouted sewer lines. Focused on the physical security implications of covert entry points created via reconnected plumbing networks (e.g., through neighboring properties) and designed defensive tools to detect and respond to such threats.

Self-Study: Subsurface Intrusion Detection via Plumbing and Tunnel Channels
Researched adversarial use of sewers, utility lines, and subterranean tunnels for covert surveillance, physical entry, and signal insertion beneath residential, institutional, or secure infrastructure.

- **Threat Model: Sewer and Utility-Line Intrusion**
  Explored how rerouted or misconnected sewer and drainage systems can be exploited by neighbors or external actors to:
  - Deploy surveillance equipment via plumbing networks.
  - Establish concealed ingress paths through wet-wall or drain-connected access points.
  - Insert harmful agents or probing signals into facility infrastructure.
- **Tool Design: Wired Camera and GPS Tracker Probes**
  Engineered deployable sensor platforms with tethered cable systems:
  - Compact surveillance modules deployable through sinks, drains, or toilets.
  - Recycled and coiled wiring for manual or motorized retraction.
  - Equipped with waterproof cameras, IR night vision, pressure/moisture sensors, and low-power RF beacons.
  - Integrated GPS-based 3D geolocation modules (using triangulation where GPS is weak) to map probe depth, lateral drift, and orientation beneath facilities.
- **Use Cases and Counter-Infiltration Strategy**
  - Detecting unauthorized access or tampering in utility channels.

  - Mapping underground routes and identifying tunnel encroachments from neighboring parcels.
  - Deploying probes as forensic devices for incident reconstruction or perimeter breach analysis.
- **Subsurface Tunnel Surveillance and RF Threats**
  Investigated techniques adversaries may use to install devices beneath critical facilities:
  - RF backscatter nodes and passive acoustic eavesdropping sensors placed in tunnels.
  - Use of EM field resonance and vibration analysis to remotely sense personnel movement or speech from below.
  - Countermeasures include ground-penetrating radar (GPR), passive RF anomaly monitoring, and seismic triangulation arrays.
- **Threat Model: Subsurface Surveillance and Access Tunnels**
  Analyzed how adversaries may create shallow or deep tunnels beneath buildings to:
  - Install eavesdropping devices directly under floors.
  - Introduce long-term passive RF probes for spectrum monitoring or signal backscatter.
  - Gain clandestine physical access for covert operations.
- **Detection Techniques:**
  - Ground-penetrating radar (GPR) sweeps and low-frequency seismic sensors to detect voids or unnatural disturbances beneath floor slabs.
  - Passive electromagnetic field mapping to identify abnormal emissions originating from tunnel-deployed electronics.
  - Vibration and audio resonance sensing to detect digging or subterranean movement.
- **Countermeasure Prototypes:**
  - Designed low-cost underground signal triangulation system using passive RF receivers and magnetic field sensors.
  - Explored shielded flooring with conductive mesh layers to block upward signal leakage.
  - Proposed AI-enhanced anomaly detection for floor-level seismic noise patterns using embedded IoT sensor arrays.

Prodeo: AI-Driven Intelligence Solutions (Launching July 2025)

Founder & Independent Researcher

- Full operational launch scheduled for July 2025 to deliver specialized AI-driven intelligence solutions across OSINT, SIGINT, cybersecurity, cognitive security, and strategic influence modeling.
- Researching transformer-based AI for real-time cyber threat intelligence, geopolitical risk assessment, adversarial influence simulations, and disinformation detection.
- Developing autonomous AI teams for narrative analysis, predictive intelligence modeling, and multi-domain influence simulations, supporting applications for government, defense, and private sector intelligence needs.
- Designing AI-powered SIGINT analysis platforms, integrating spectrum monitoring, SDR-based signal intelligence, and anomaly detection in RF environments to monitor adversarial communication and detect covert transmissions.
- Engineering AI-enhanced forensic cybersecurity systems for end-to-end monitoring—including system logs, TCP/IP network traffic, firmware integrity checks, and anomaly detection across all OSI layers.
- Researching hyperbolic transformer-based techniques to protect sensitive physical documents from adversarial EM/radiation-based document espionage (terahertz/zeta wave scanning, backscatter imaging). Developing AI-assisted shielding using metamaterials and dynamic electromagnetic interference (EMI) cloaking.
- Combining AI-augmented OSINT automation, psychological operations (PsyOps) modeling, and cognitive warfare research into real-time narrative analysis engines to predict and counter adversarial influence operations.
- Innovating in multimodal environmental sensing, integrating WiFi human pose estimation, ultrasound radar from mobile devices/IoT speakers, and RF/EM fusion for privacy-preserving surveillance countermeasures, real-time healthcare monitoring, and polygraph-integrated security screening technologies.
- Expanding capabilities in **polygraph-integrated transformers**, developing multimodal AI systems that combine RF, ultrasound, and bio-sensing technologies to enhance real-time deception detection, behavioral profiling, and physiological monitoring for security applications. These systems establish a dynamic baseline of physiological and neurophysiological markers, enabling AI-driven anomaly detection in speech patterns, microexpressions, heart rate variability, and stress-induced autonomic responses. By leveraging transformer models trained on cognitive state estimation and adversarial deception modeling, this framework translates physiological fluctuations into interpretable cognitive states, reconstructing **internal voice, thought flow, and decision-making processes** in real time. The system synthesizes sensory inputs to infer **implicit reasoning patterns, subconscious hesitations, and response formulation dynamics**, offering an AI-assisted cognitive forensics tool for high-stakes security screening and adversarial interrogation scenarios.
- Researching laser-based Non-Line-of-Sight (NLoS) imaging (e.g., reconstructing rooms through keyholes) and its countermeasures, including hyperbolic-transformer-based anomaly detection and smart architectural shielding for SCIFs and executive spaces.
- Exploring plasma and EM-based propulsion and defensive systems for underwater, subsurface, and aerospace security—applying this to quiet submarine propulsion, subsurface defense against tunneling threats, and counter-space applications.
- Investigating next-generation projectiles (terrain-penetrating munitions) and developing gravitational wave

and neutrino-based sensing techniques to detect and map subsurface threats—advancing dual-use capabilities for both strategic deterrence and scientific sensing.
- Researching adversarial applications of **radiation-based espionage countermeasures**, including AI-enhanced detection of unauthorized scanning technologies used to extract information from printed documents, integrating these into secure office designs and SIGINT counter-surveillance operations.
- Applying structured analytic techniques (SATs), cognitive warfare methodologies, and AI-enhanced deception detection across all intelligence domains—integrating these into a unified AI decision-support platform for intelligence-driven operations.
- Actively developing proprietary LLM-based AI agents trained directly on the intelligence cycle (Heuer's structured analysis, HUMINT/SIGINT/OSINT fusion), enabling rapid sensemaking, red teaming, and adversarial simulations in both government and private sector environments.
- Preparing Prodeo to offer consulting, technology development, and AI-enhanced analytical solutions for national security clients, defense contractors, technology startups, and private sector organizations requiring intelligence automation, adversarial modeling, and strategic influence analysis.

Teaching & Leadership

University of Arizona (2022–Present): GTA for College Algebra/Calculus.

San Francisco State University (2019–2022): GTA for Calculus, focusing on proof-based exploration.

Awards & Certifications

- Protecting God's Children Online Awareness 4.0 – Order of Malta (March 2025)
- Nominated for MSRI Summer School, Oxford (Metric Geometry, 2021)
- Information Security Awareness & Safety Training, Univ. of Arizona (2023)
- MASS Scholarship, Penn State (Full Tuition, 2017)
- ACM SIGMOD Service Award (2016)
- Big Data Training, MIT CSAIL (2015)

Technical Skills

Programming & Tools: Python, C/C++, Java, Lisp, R, Mathematica, Shell, Lean 4, Git/GitHub, LaTeX.

Cybersecurity & OSINT:
AI-assisted network forensics, AI-driven anomaly detection in TCP/IP traffic, firmware-level intrusion detection, reverse-engineering network threats, cryptanalysis, penetration testing via transformer models.

System & Network Security: TCPDump/Wireshark analysis, intrusion detection, monitoring firmware/memory vulnerabilities, reverse-engineering Intel AMT and similar architectures for anomaly detection.

Mathematical & Computational Methods: Real/complex analysis, measure theory, topology, functional analysis, stochastic processes, encryption/decryption, HPC, advanced cryptography.

Radio Frequency (RF) & SIGINT: Spectrum analysis, Software-Defined Radio (SDR), RF signal detection, FCC amateur radio exam preparation.

AI-Enhanced Intelligence & OSINT:
AI-driven intelligence automation (Heuer-based LLM agents), adversarial social engineering defense, NLP-driven deception detection, multi-agent data fusion for SIGINT/HUMINT integration.

Volunteer and Community Engagement

- University of Arizona Tucson Math Circle (Oct 2023 – Present) Maintaining the website to support outreach and mathematical education.
- Poverello House (Feb 2025 – Present) Volunteering to assist the homeless community with hands-on support.
- Knights of Columbus Blood Drive (Mar 2025, upcoming) Providing service at a local blood drive event at St. Thomas the Apostle Parish.
- Math Circle Teaching Assistant – University of San Francisco (Spring 2017) Provided mentorship and mathematical enrichment to young students.
- Hospital Volunteer – Taipei, Taiwan (2000 – 2006) Assisted elderly patients and children with disabilities through direct service.
- Altar Server – Fu Jen Catholic University (1998 – 2003) Assisted in liturgical celebrations attended by university faculty and students.

Additional Information

Faith: Catholic (Confirmed 28 years). Knight of Columbus (CUF exemplification completed). Completed *Protecting God's Children Online Awareness 4.0* (March 2025) under the Order of Malta for safeguarding minors and vulnerable individuals.

Languages: English (Fluent), Mandarin/Taiwanese (Native), Learning Latin, French, Spanish, Italian, Hebrew

Memberships: Pi Mu Epsilon Honor Society (University of San Francisco)

References: Available upon request