



Advanced Cyber and AI Security Leadership Certificate Program

An Applied, Governance-First Cybersecurity and AI Leadership Program Delivered with BMCC and Independently Certified by the CSOAI.

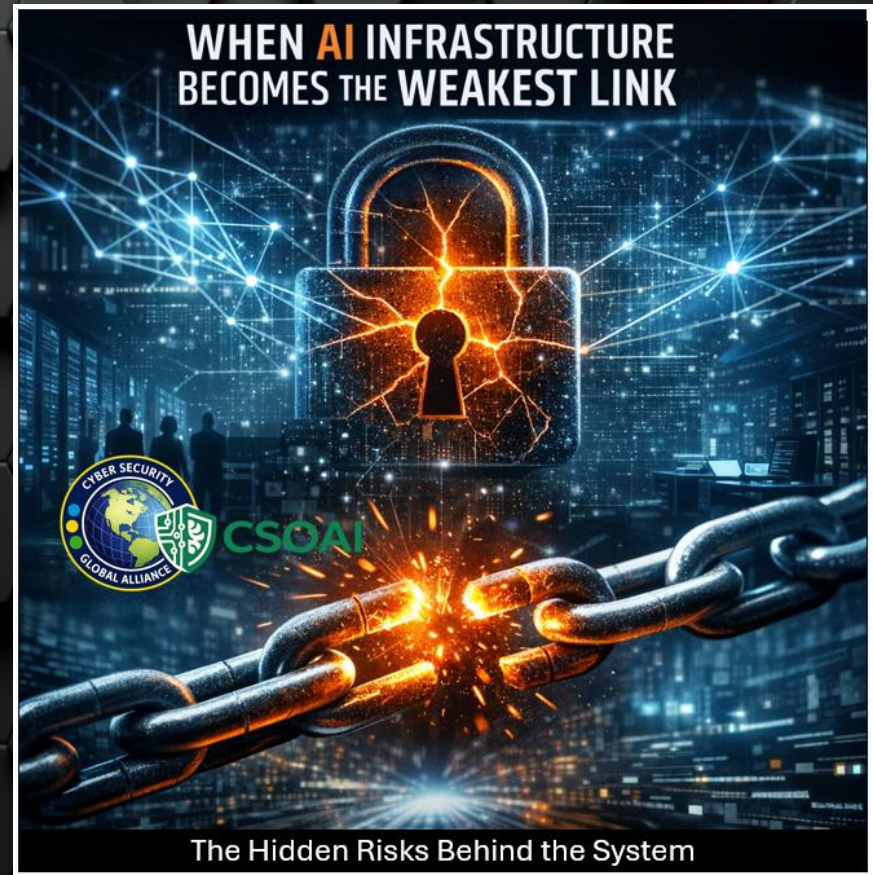
The Reality We Face

Cyber and artificial intelligence failures are no longer primarily technical.

They are failures of leadership governance and judgment.

- Cyber and AI risks now directly impact national security economic stability and public trust
- Most major incidents exploit human decision making and governance gaps not technology alone
- Organizations need leaders capable of accountable decisions not just technical operators

The weakest link is no longer infrastructure. It is leadership under pressure.



Why Cyber and AI Leadership Matters

Technical tools alone cannot prevent system failure

Leadership decisions determine outcomes under pressure

- Cyber and AI leaders must make defensible ethical decisions in real time
- Accountability and judgment matter more as systems become more automated
- Artificial intelligence amplifies both organizational capability and risk simultaneously

Effective leadership is the difference between resilience and failure in high-consequence environments.



James Castle, CEO & CSO



Dr. Chris Golden, PRES & COO

CSGA WhiteHat Institute for Cyber, AI, and Strategic Security

Introducing the WhiteHat Institute for Cyber, AI, and Strategic Security

The WhiteHat Institute prepares leaders for environments where cyber and artificial intelligence failures have real world consequences.

- Governance-first education model built for accountability and trust
- Designed specifically for high-consequence national and critical environments
- Grounded in ethics law and decision authority not tools alone

This is not a technical training program. It is a leadership institute for cyber and AI responsibility.



Flagship Credential

Advanced Cyber and AI Security Leadership Certificate

A governance-driven professional credential designed for high-responsibility cybersecurity and artificial intelligence leadership roles.

- Developed in partnership with BMCC Center for Continuing Education and Workforce Development
- Independently certified to ensure credibility integrity and accountability
- Designed for experienced professionals and emerging leaders in high-consequence environments

This credential signals readiness to lead cyber and AI decisions where trust responsibility and impact matter.



CSGA WhiteHat Institute for Cyber, AI, and Strategic Security

Program Architecture

The WhiteHat program is structured to balance flexibility rigor and accountability while supporting real world professional schedules.

- Modular and stackable design allowing progressive skill and leadership development
- Structured to be completed in under two years while maintaining high standards
- Mastery gated progression ensuring advancement only through demonstrated competence

Learners advance by proving readiness not by accumulating time or credits.



CYBERSECURITY WHITEHAT PROGRAM
U.S. Department of Commerce Endorsed

COURSE FEATURES

- Diplomatic Cyber Leadership
- Apprenticeship Program
- Books and Materials Included
- Certificate with Certification
- Job Placement Upon Graduation
- CompTIA Security+ Certification
- 100% Fully Mentored
- 100% Fully Online
- No Travel Required
- WhiteHat with Certified AI Analyst
- Financial Assistance Available if Needed
- Learn at Your Own Pace
- No International Student Rates

LEARN IN-DEMAND SKILLS AROUND YOUR SCHEDULE

The WhiteHat learning model integrates advanced tools with human oversight to ensure rigor accountability and defensible outcomes.

POPULAR COURSES INCLUDE

- Analyze Remote Intrusion Attempts
- Investigate Watering Hole Attacks
- Examine a Compromised Hosts' Memory
- Conduct a Forensic Disk Examination
- Close Your Investigation
- Exploit a Website
- Entrepreneurship Program
- Threats, Attacks and Vulnerabilities
- Cyber Sleuth K-12 Digital Program
- Cyber Defense and Cyber Attack, and Cyber AI Research Institute
- CompTIA Security+ Certification (8 weeks, time depends on students skill)
- AI and Business Modules
- Identity and Access Management
- Architecture and Design
- Certified AI Analyst (200-hours)
- AI-Assisted and Human-validated
- \$8,000 Inclusive Program

To learn more and enroll, visit:
<https://bmcc-cyberprogram.com>

Phase 1

CompTIA Security Plus Certification

Phase 1 establishes a shared professional foundation and common security language for all participants.

- Industry recognized baseline cybersecurity certification
- Ensures consistent technical understanding across cohorts
- Delivered fully online and designed for working professionals

This phase creates a common starting point. Leadership development begins in the phases that follow.



CSGA WhiteHat Institute for Cyber, AI, and Strategic Security

Phase 2

WhiteHat Core Program

Phase 2 is the foundational leadership curriculum of the WhiteHat Institute, focused on real-world cyber and AI risk in national and critical environments.

- Advanced cyber defense principles applied to high-consequence scenarios
- Direct focus on national security and critical infrastructure systems
- Ethics law and governance embedded throughout all instruction and assessment

This phase trains participants to operate where cyber and AI decisions carry strategic legal and societal consequences.

NEW RISE IN NATION-STATE GREAT POWER COMPETITION UNRESTRICTED WARFARE IN THE GRAY ZONE VIA 'NO RULES'

THE MODERN BATTLEFIELD IS EVERYWHERE

TOP EXISTENTIAL RISK TO U.S. COMPANIES, UNIVERSITIES, AND NATIONAL SECURITY

NON-MILITARY

Economic Warfare*
Financial Warfare*
Business Warfare*
Trade Warfare*
Resource Warfare*
Regulatory Warfare*
Legal Warfare**
Education Warfare*
Smuggling Warfare*
Media Warfare**
Propaganda Warfare
Culture / Race Warfare
Ideological Warfare
Religious Warfare
Poisoning Warfare
Environmental Warfare

TRANSITIONAL

Espionage Warfare*
Information / Cognitive*
Intelligence Warfare*
Influence Warfare*
Resource Warfare*
AI / Big Data / Quantum*
DarkNet Warfare*
Technology Warfare*
Cyber Warfare*
Political Warfare*
Drug Warfare*
Infiltration Warfare*
Industrial Warfare*
Psychological Warfare**
Diplomatic Warfare
Subversion Warfare

MILITARY

Biological Warfare
Chemical Warfare
Ecological Warfare
Space & EMP Warfare
Electronic Warfare
Guerrilla Warfare
Terrorist Warfare
Conventional Warfare
Kinetic / Smart Warfare
Nuclear Warfare

AKA: 'HYBRID WARFARE'

- Espionage & IP Theft: Core focus of UHW
- Infiltration & Subversion: Key objectives
- Cyber Warfare: Key accelerator to all UHW
- Over 100 Methods of Hybrid Warfare
* Related to Economic and Transaction Warfare
** The CCP Three Doctrine Warfare



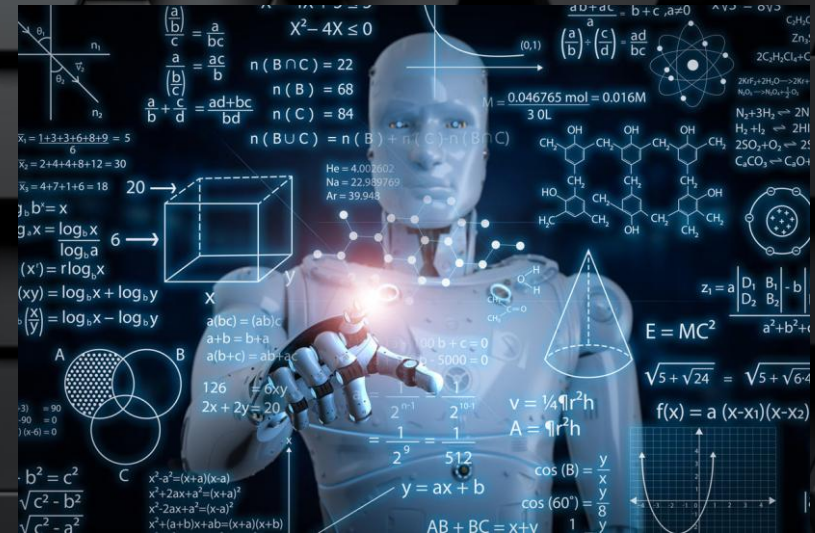
Phase 3

Certified AI Analyst

Phase 3 develops disciplined expertise in artificial intelligence systems with a focus on risk governance oversight and accountability.

- Analysis of AI architectures decision models and system dependencies
- Governance auditability and risk management for AI enabled systems
- Responsible AI deployment aligned with legal ethical and societal expectations

This phase prepares leaders to assess control and govern AI systems rather than simply deploy them.



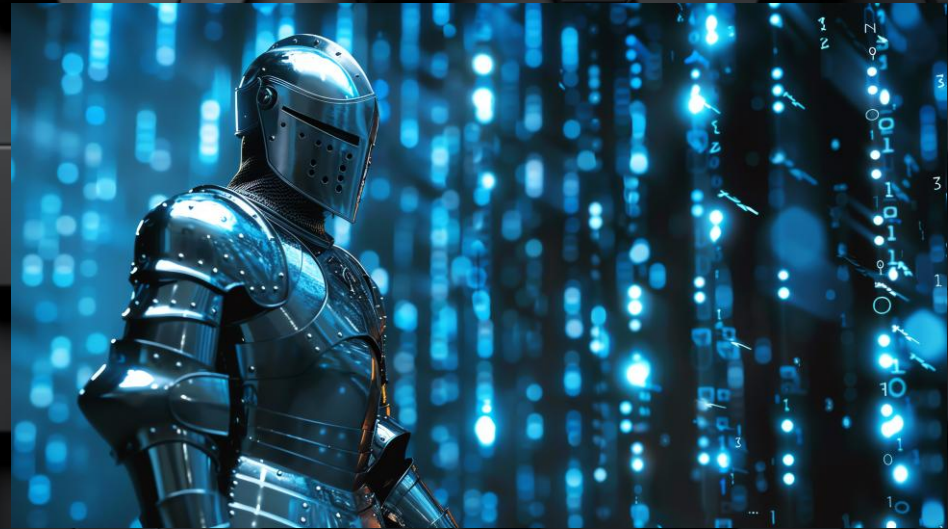
Phase 4

Diplomatic Cyber Leadership

Phase 4 develops the leadership and communication skills required to manage cyber and AI risk across institutions sectors and jurisdictions.

- Strategic communication for high-pressure cyber and AI incidents
- Coordination across public private and international stakeholders
- Ethical conflict de-escalation and trust preservation in contested environments

This phase prepares leaders to govern cyber and AI crises where technical fixes alone are insufficient.



Phase 5

Online Apprenticeship

Phase 5 integrates applied practice with faculty oversight to reinforce accountability judgment and professional readiness.

- Structured applied workforce experience aligned to cyber and AI governance
- Faculty supervised projects with documented learning outcomes
- Delivered fully remote to support global and working professionals

This phase bridges education and real-world responsibility under supervised conditions.



Program Pathway

The WhiteHat program follows a structured progression from foundational knowledge to leadership responsibility and applied practice.

Security Plus →
WhiteHat Core →
AI Analyst →
Leadership →
Apprenticeship →
Certificate

Each stage builds on verified mastery, reinforcing accountability, judgment, and readiness for high-consequence cyber and AI environments.



Learning Model

The WhiteHat learning model integrates advanced tools with human oversight to ensure rigor, accountability, and defensible outcomes.

- AI assisted learning used to enhance analysis scenario exploration and feedback
- Human validated outcomes through faculty review and structured assessment
- Audit ready evaluation designed for transparency consistency and institutional trust

Technology supports learning. Accountability remains human.



Governance and Trust Model

The WhiteHat Institute is structured to ensure accountability credibility and independence across education governance and certification.

- CSGA governs mission ethics and strategic oversight
- BMCC delivers accredited instruction and academic operations
- CSOAI provides independent certification and credential issuance

This separation of roles ensures transparency accountability and public trust in all program outcomes.



Certification Integrity

WhiteHat certifications are designed to maintain credibility trust and long-term value across public private and international environments.

- Evidence based assessments tied to demonstrable competencies
- Time bounded credentials requiring continued relevance and accountability
- Issued independently to preserve integrity and prevent conflicts of interest

Certification represents verified capability and ethical responsibility, not attendance or time served.



Ethics and Accountability

Ethical leadership and accountability are foundational requirements for cyber and artificial intelligence professionals operating in high-consequence environments.

- Mandatory code of ethics governing professional conduct and decision making
- Auditable enforcement mechanisms with documented accountability processes
- Designed to protect public trust institutions and democratic systems

Authority in cyber and AI comes with responsibility. Trust must be earned and maintained.



Student Outcomes

Graduates of the WhiteHat Institute demonstrate readiness to operate responsibly and effectively in cyber and AI environments where consequences matter.

- Demonstrated technical competence aligned with industry and governance standards
- Ethical judgment supported by defensible decision-making frameworks
- Leadership maturity appropriate for high-consequence professional environments

Graduates are prepared to contribute with accountability, judgment, and institutional trust.



Career Pathways

The WhiteHat program prepares graduates for a range of professional roles where cyber and artificial intelligence governance expertise is required.

- Cybersecurity analyst supporting defense enterprise and critical systems
- AI security analyst focused on risk governance assurance and oversight
- Governance policy and compliance roles across public and private institutions

Career pathways reflect areas of professional applicability rather than guaranteed outcomes.



Affordability and Access

The WhiteHat Institute is designed to expand access to advanced cyber and AI leadership education without compromising rigor or standards.

- Structured to reduce financial and logistical barriers to participation
- High academic and professional rigor delivered at sustainable tuition levels
- Broad access across regions and backgrounds without dilution of requirements

Access is expanded while expectations remain uncompromised.



CSGA WhiteHat Institute for Cyber, AI, and Strategic Security

BMCC Advantage

Partnership with Borough of Manhattan Community College anchors the WhiteHat Institute within a trusted public higher education framework.

- Public higher education credibility with established academic governance
- Direct alignment with workforce development and real-world skill requirements
- Institutional trust supporting transparency accountability and long-term program sustainability

BMCC provides the academic foundation that ensures rigor legitimacy and public confidence.



BMCC Cybersecurity WhiteHat Online Program

BMCC Cybersecurity WhiteHat Program

Secure the Future. Lead the Change.

Why Choose This Program?

- 43-week online program designed for global careers.
- Fully mentored training with real world cyber defense experience.
- CompTIA Security+ Certification Included
- Job placement guaranteed upon graduation

Program Highlights

Format: 100% online, no travel required.
Schedule: 25 hours / week, learn at home
Start Date: January 5, 2026

Contact & Registration

diplomacy@bmcc.cuny.edu | bmcc-cyberprogram.com

What You'll Learn

- Cyber Defense & Attack Strategies
- Reverse Engineering & Forensics
- Threat Analysis & Vulnerability Management
- Quantum Encryption & Resilience
- Insider Threat & SOC Operations

Your Benefits

- Certificate of Completion
- 5-Year Membership in Cyber Security Global Alliance (CSGA)
- Global Cohorts & Regional Mentorship Opportunities

CYBERSECURITY WHITEHAT PROGRAM
U.S. Department of Commerce Endorsed

COURSE FEATURES

- Global Cohorts, Regional Mentorship Opportunities
- 24/7 Access
- Books and Materials Included
- Certificate of Completion
- Job Placement Upon Graduation
- CompTIA Security+ Certification
- 100% Fully Mentored
- 100% Fully Online
- No Travel Required
- Security Vetting Program
- Financial Assistance Available if Needed
- 25 Hours Per Week, Learn at Home
- No International Student Fees

LEARN IN-DEMAND SKILLS AROUND YOUR SCHEDULE

Offered in partnership with Toranowasa Aerospace and Defense Group and Cyber Security Global Alliance, our online Cybersecurity Whitehat Career Training is designed to prepare you for immediate entry or advancement in cyber security and cyber defense career opportunities globally.

POPULAR COURSES INCLUDE

- Analyze Remote Intrusion Attempts
- Investigate Watering Hole Attacks
- Examine a Compromised Host's Memory
- Conduct a Forensic Disk Examination
- Close Your Investigation
- Exploit a Website
- Insider Threat?
- Threats, Attacks and Vulnerabilities
- Cyber Sleuth and Immediate Immersion (8 weeks, 120 hours)
- Cyber Defense and Cyber Attack, Reverse Engineering (15 weeks, 375 hours)
- CompTIA Security+ Certification (8 weeks, time depends on students skill)
- AI and Business Modules
- Identity and Access Management
- Architecture and Design
- Cryptography and Quantum
- Cyber Range and Online Testing

To learn more and enroll, visit: <https://bmcc-cyberprogram.com>

Ready to launch your cybersecurity career? Join the BMCC Cybersecurity WhiteHat Program and gain the skills, mentorship, and certification you need to succeed in one of the fastest-growing fields worldwide. This 43-week fully online program includes Cyber Defense, Cyber Offense, Immediate Immersion, CompTIA Security+ Certification, and hands-on training with guaranteed job placement upon graduation. Don't wait, Secure Your Future and Lead The Change!

Email: diplomacy@bmcc.cuny.edu

More Info: +1 (212) 346-8433

Website: bmcc-cyberprogram.com

Community and Impact

The WhiteHat Institute is designed to serve public institutions professional communities and global stakeholders responsible for cyber and AI security.

- Anchored in New York City with direct access to public sector and industry ecosystems
- Globally relevant curriculum addressing cross-border cyber and AI risks
- Public service mission focused on trust safety and institutional resilience

The program strengthens communities by preparing leaders to protect systems people and democratic institutions.



In Closing



Secure the future. Lead with integrity.

The WhiteHat Institute prepares leaders to govern cyber and artificial intelligence systems where trust responsibility and public impact are inseparable.

James Castle
Global Chairperson
Cyber Security Global Alliance
CSGA Cyber AI Research Institute
Center for the Safety of AI

csga-global.org
bmcc-cyberprogram.com
csoai.org

chairperson@csga-global.org