1G CYBER

Gangs & Delinquent Youth Avoidance
Cybersecurity Education for Social Transformation (EST)
in New York City and State

Dr. Dustin Fraser, CASP+, SSCP

Vision: The vision of this program is to create clear incentives, core education, institutional knowledge, strategic focus on vulnerable youths, and training pathways that lead to cyber security apprenticeships and jobs.

Mission: To provide cyber security apprenticeship and work opportunities for vulnerable people through education for social transformation.

Action Plan:

1. Bring stakeholders together, starting with small but core groups, then branching out with backstopping strategy
2. Provide resources to implement programs using combined expertise
3. Establish civic leadership commitment, duration, and scope of engagements
4. Examine advanced research and practice among team members to engage stakeholders strategically, tactically, and operationally
5. Put proposals into action measuring performance and effectiveness reviewed monthly

Background: The increase in financial and payment fraud has caused a significant economic impact to business and society. The constant data breaches across New York enervates organizations' ability to recover after an incident. The slow recovery has a direct impact on the overall economy and profit growth. The root cause of these issues is the lack of a cybersecurity workforce with the requisite knowledge, skills, and abilities to securely implement and operate essential infrastructure and digital services.

To protect future growth, programs must be implemented to find skilled professionals from a diverse population of young and eager cyber operators. A program that develops advanced cybersecurity capabilities through the lens of a socio-technical system will address the issue from the ground up. Sociotechnical systems (STC) underpin our society but combining this with Education for Social Transformation (EST) will ensure that the mission of combatting cybercrime has the appropriate goals and objectives, processes and procedures, cultural changes, and advanced understanding of relevant technology.

The proposition of combining STC and EST ensures that citizens are not impacted by cybercriminals while a new population of cyber professionals leverages advanced training and tools to drive high situational awareness. The training program that first accomplishes this creates a talent pipeline essential to protecting critical infrastructure in New York City and State. The population required for this program must be diverse, ensuring opportunities for all ages and allowing the identification of top talent. This approach is essential because top talent could otherwise be missed if closed to any group or location.

Geographic Location:

a) **Priority 1:** Brooklyn, Bronx, Queens, Staten Island
b) **Priority 2:** Surrounding Cities
c) **Priority 3:** State

Demographic:

a) Youths inclined to Gang Violence and Warfare
b) Young women
c) Vulnerable Adults and Youth
d) Immigrant and Refugee (all ages)

Objective:

1. Overview of the work of Lambeth's police proactive and gangs' team, how police work in partnership with others to address anti-social behavior including gang violence, exploitation of children, by providing community support at a neighborhood and national education level.
2. Set global standards for the skills to secure online transactions.
3. Recruit financial services employers in support of the City the same time as positioning 1GCYBER and partners at the heart of skills partnerships.
4. Advance the importance of security by design for information technology and infrastructure work roles through National Initiative for Cybersecurity Education (NICE).
5. Develop soft skills through extra-curricular creative arts and sports activities for participants participating in proposed technology programs.
6. Put forward advances from research and practice internal and external to the City

Purpose:

Education for Social Transformation (EST) can improve economic and social dispositions which leads to regional change even if the perceived values do not readily provide a return on investment. Several barriers to youth workforce upskilling exist, of which, the top challenges are the lack of time, budget, interest, and structure to support various curriculum delivery programs.

Cyber security Education Opportunity Matrix:

TACTICAL	**OPERATIONS**	**STRATEGIC**
PROBLEM CHARACTERISTICS	DESCRIBE PROBLEM	PROBLEM ENVIRONMENT
Vulnerable Youths	Technical and Vocational Training	Apprenticeships
Gang Warfare and Violence	Employment Pipeline	Measurable Outcomes

Cyber security Education Performance Matrix:

Cost per Delivery	Measures of Effectiveness & Measures of Performance	Economic and Social Change
Current Central Tendencies (Metrics)	Virtual and Physical Resources & Time	Target State of Increased Youth Employment and Reduced Violence

Local Partner Matrix:

LOCAL	MISION	FOCUS
High School	Sector-based Work Programs	Cybersecurity and Technology Talent Pool and Ecosystem as proposed by Dr. Fraser's framework.
Department for Work and Pensions	Support Employment Programs	
Colleges	Soft Skills	
Specific Institutions	Advance Women Professionals	
Vocational	Co-education Opportunities	
Local State Schools	Education Opportunities and Talent Pool	
Churches	Religion, Outreach and Youth Facility	

A strategy for differentiation must include youth workforce skills development. This strategy helps organizations obtain diverse talent to fill cybersecurity roles and responsibilities. The potential practitioners must pursue these careers with academic rigor to obtain advanced capabilities vital to protecting critical infrastructure with high situational awareness.

1G CYBER

Education for Social Transformation/Sociotechnical Systems – Cybersecurity Professional Upskilling Program Objectives:

The below cybersecurity objectives are high-level targets to be accomplished through an integrated approach to social and economic development.

Goal	**Training and Support aligned with:** 1. Industry: COMPTIA, ISC2, ISACA, CyberSec First Responder 2. National Institute of Standards and Technology (NIST) 3. Federal Financial Institutions Examination Council (FFIEC) 4. ISO/IEC 27001 5. Cyber Resilience Review		
Executive Support: • Cyber Strategy • Decision Making • Governance Roadmap	Unlimited	Unlimited	Unlimited
Business Teams: • Technology Solutions • Information Assurance • System User Analysis	Unlimited	Unlimited	Unlimited
IT Infrastructure: • Identity and Access • Configuration and Change Management • Vulnerability & Remediation • Incident Response	Unlimited	Unlimited	Unlimited

Cyber Organization: • Program Integrity	Use the frameworks to begin or benchmark organizations’ current state	Advance maturity from baseline to innovation by exploring existing gaps in risk management	Leverage audit capabilities and control families to develop robust cybersecurity programs
Minority Communities: Advance Education	Tailor cybersecurity training programs for skills development and job placement	Advance economic and social well-being of communities and people	Explore complex phenomenon, such as gang violence and warfare, to advance intrinsic value civic education

Local and national resilience can be achieved through a workforce capable of applying tacit and codified cybersecurity knowledge, skills, and abilities to job duties. Today’s organizations encounter many workforces’ challenges when developing their governance roadmaps. These include identifying current and target operational needs, receiving unbiased assessments, and developing intrinsic outcomes. To address this problem, a robust cybersecurity workforce must possess advanced technical skills and non-technical capabilities.

Proposed Training:

Training Population	**Programs**			
Business	Cybersecurity Analytics	Incident Response	Audit and Risk Management	Security Testing
Administration	Awareness Training	Identity & Access Management	Security Incident & Event Management	Vulnerability & Remediation
Operations	Linux Administration	Network Administration	Systems Administration	Computer Security
	Threat Intelligence or Informed Defense	Cyber Investigations	Situational Awareness	Cyber Orchestration

Proposed Team:

Name	Experience
Dr. Dustin Fraser, CASP+, SSCP	Academia, and Industry
Private Member	Academia, Government, and Industry
Private Member	Academia, Government, and Industry