A Holistic and Sustainable Approach towards Comprehensive Cybersecurity for Africa by Essoka Cybersecurity Division (ECSD) – *An ECSD Partner4Africa Project*.

After over 18 years of security, Essoka Security Company (www.essokasecuritycm.com) innovated Essoka Cybersecurity Division (www.essokacybersecuritydiv.com), via a share of BTH Education Group's International Corporation Development Program (www.btheducationgroup.org) for Essoka Corporation, to harness a more comprehensive definition of security according to the age (the Digital and Information Security Age).

Standardization

Therefrom, ECSD (Essoka Cyber Security Division) has accomplished international accreditation and recognition for training and proctoring cybersecurity exams ***(Cert ID EATC52208)*** through EC-Council, as a premier international standardization framework embodying her vision on cyber-information security throughout Cameroon and across Africa.

Our Vision

Putatively, time would fail us to contract or enumerate a compendium of cybersecurity threads; cybercrimes and information warfare (TJX credit Card Hacks - 2007 (Records Breached: Data from 94 million customers), Heartland Payment Systems - 2008 (Records Breached: Information from over 100 million cards), NARA - 2009 (PII of 70 million members of the military), Sony Entertainment Network - 2011(Data of 100 million customers), TARGET - 2013 (Records Breached: 40 million customers that costed the company more than $116 million), Google Play hack, eBay Data breach, Home Depot Data breach – 2014, Anthem Healthcare – 2015 (Records Breached: Data for about 80 million health insurance customers), Feb 2016 - US Department of Homeland Security (DHS) and Federal Bureau of Investigation (FBI) attacks (hacktivist published personal information (names-titles, job descriptions, email addresses and contact information) of approximately, 9000 DHS employees and 20 000 FBI employees); years of mega breaches impacting, government agencies, retail and financial institutions etc.), Malware trends and threats (Defacement Trojans, Botnet Trojans, ICMP Tunneling, Virus Hoaxes and Fake Antiviruses, Ransomware), Types of attacks on systems, Social Engineering (Human-Computer based Social Engineering, impersonation, identity theft), DoS/DDoS, application and network level session hijacking attacks, SQL injection attacks (Error-based, blind, union, etc.), Mobile Platform Attack Vectors, Security Frameworks (information security controls, Information Assurance (IA), Management Programs, Threat modeling, Enterprise Information Security Architecture (EISA), Defense in Depth, Physical security controls, security policies, laws and standards, Security pertaining to Cloud and IoT).

Security challenges in the age seem aeonian to governments, organizations, institutions (including professional institutions of the art), Universities of renown, and to the global citizenry at large; the need to coordinate policies, develop systems and virtuoso, to apprehend and manage the framework of this era (the digital era), outsizes the dispensation.

Moreover, the geometry and nature of cybercrimes, hacktivists, Blackhat Hackers, divulge the exiguity by solution providers (training, certification organizations or institutions) to the cyber-information security framework and the need for governing policies on cybersecurity to circumcenter on the integral, juristic aspects:

How do we avoid cybercrime? – Our Formation Concept
If criminology nominates demeanor (behavioral attributes) as the basis of crime, cyber criminology would espouse the same because the focal thread is crime;
Any training, certification program or degree that indeed lauds professionalism as the possession of skills from fundamental to advanced skills, without focusing on one and or all of the personal development traits, highlighted by UDHR Article 26 part 2, isn't merely exiguous to the digital age and security challenges, but as a matter of fact, constitutes the most wicked problems pertaining to the global security landscape: A Trained criminal!

The Dynamics of Our Formation Concept
What is the global focus on the war on cybercrime?

Stopping the criminal and the crime
Whitehats or ethical hackers work in government agencies, companies and organizations to prevent cybercrimes. Criminals of cyber breaches (say, Blackhats or cyber-criminals) are apprehended and their crimes brought to a halt, after unredeemable damages. Meanwhile, a lot of resources are dedicated to penalization and recovery of damages, little or no effort is made to comprehend the hypostasis of the crime.

Preventing the criminal and the crime
A sustainable approach is the nonpareil methodology to fight cybercrime – a preventative disposition that considers the more in-depth aspects; on the other hand, defense in depth in cybersecurity is a security strategy in which security professionals use several protection layers (Policies, Procedures, and awareness – Physical Security-Perimeter Security-Internal Network-Host-Application-Data), adopted from the military principle that it is more difficult for an enemy to defeat a complex and multi-layered defense system than to penetrate a single barrier.

However, shouldn't the aforementioned technical delineation of defense in depth be a part of a more integral, clogging holism; one that could hypostasize

cybercrime to the nonoccurrence of the full development of the human personality – UDHR 26 part 2.

Formation Concept (I-ICDP)
Mental, emotional, temperamental and behavioral development are the only exclusive traits of personality and the juristic framework of the full development of the human personality, as the genius loci of all development vertices – A/RES/41/128, Article 2 part 1.

Our objective and vision within the formation program is to identify by law, the legal environment for education for sustainable development (consentient with DESD) of a genius program in cybersecurity and consequently, build genius teams of technocrats; a genius team building program of technocrats throughout Cameroon, across African et al – mentally, emotionally, temperamentally and behaviorally apt (possessing striking appropriateness and pertinency) to provide the most comprehensive information/cybersecurity services, consolidated by the governing definition of education: an education that encompasses personal, postindustrial and recondite organizational development, within a critical action learning environment (CAL-E).

I-ICDP: – Technical details and standards of the Formation programs
Technical details under the postindustrial aspects of the formation program, cover an integral, across-the-board wad of certifications from fundamentals-beginner, through intermediate to advanced certifications, from notable providers in the industry of information and communication technologies and cybersecurity, such as Certiport, CompTIA, and EC-Council.

Therefore, the virtuosity of the aforesaid Formation program is not only accomplished by an all-inclusive design that covers the developmental period of a virtuoso (with a well-knit, greater focus on fundamental or novice strategic certifications to carter for the requirements of advanced-expert certifications that opportune the cogency of such an education to the age (digital and information security era) for all, concordant with an education for all : EFA - UNESCO), but is altogether, consentient with the most elevated international standards as exemplified below;

Postindustrial Certifications for ECSD Tech Training Program:

1st Tier: 2 Month – A recondite Focus on Fundamentals

- Digital Literacy (IC3)
- CompTIA IT Fundamentals – Introduction to the world of IT
- End-User Cybersecurity Certification (Certified Secure Computer User- CSCU)
- ECSS (EC-Council Certified Security Specialist) – Introduction to the world of information security.

- Linux and C++ Programming Experience Program
- **Ethical Hacking:** Introduction to CEH… (5 Days Class, comprehensive introduction)

2nd Tier: 6 months
- CompTIA A+ (Information technologies Certification)
- CompTIA Network+, (Networking, Communication technologies)
- Certified Network Defender (CND) - Beginner
- Introduction to Programming Languages for Hackers: 1st Module - Web Hacking (Module, guided notes, facilitation, research-w3 school and other support systems)
- CND – Intermediate & Advanced Program
- CEH BEGINNER/NOVICE Program
- CND Exam

3rd Tier: 3 months
- CND CAL-E (CAL-E of 2nd Tier)
- Programming Languages for Hackers: 2nd Module - Exploit Writing
- CEH INTERMEDIATE Program

4th Tier: 3 Months
- CompTIA Security+
- Programming Languages for Hackers: 3rd Module - Reverse Engineering
- CEH ADVANCED Program

5th Tier: 4 Months
- CEH EXPERT Program
- CEH Exam

6th Tier: 1 Months
- CEH Critical Action Learning Environment (CAL-E)
- **Cyber Forensics:** Forensic Investigation Fundamentals (CHFI)
- **Introduction to Security Analyst Certification** – ECSA

7TH Tier: 3 Months
- CEH Critical Action Learning Environment
- Forensic Investigation intermediate program (CHFI)
- Advanced CHFI
- CHFI Exams

8TH Tier: 3 Months
- CEH CAL-E
- CHFI CAL-E
- ECSA-1
- ECSA-2
- ECSA Exams

9TH Tier
- Critical Action Learning Set
- Critical Action Research
- Critical Action Learning

10th Tier: Continuous Education Programs – LPT Master Special Path

What are the underlying goals of all developmental isms, covered by this platform?
Our way of doing Cyber (Our Hallmark) – What does BTH Education Group's ICD program appertaining to International Education and Development highlight?

As the world's Leading International Education and Development organization, BTH Education Group's ICD has keynoted ECSD's Formation program as nonpareil via the application of the most comprehensive sustainable international education and development framework; a cardinal personal development path that encompasses all redolent aspects of systemic development such as, apprehension, value and value systems, theory of knowledge, and systemics.

This keynote move by ECSD is the most sustainable development of information security framework to unriddle the issues of the age!

The wad of records of breaches throughout the decade including arcane governmental agencies like DHS and FBI and a series of multinational corporations, solely bespeaks a declension towards securing the information assets, structures, and the architecture of the digital era.

A lot of training is going on and training and certification institutions are innovating on what is considered relevant to secure the age, and succeeding too soon without attention to or the development of the finer nuances – the full development of the human personality.

The full development of the human personality (mental, temperamental, emotional and behavioral development) via the international machinery on education and development (UDHR Article 26 part 2 & A/RES/41/128), is the lawful direction of education, in all her facets, features, spheres, sectors and perspectives.

All nonaccomplishments or nonperformances, and all accomplishments and performances of the digital age pertaining to information, communication technology and cyber or information security are contingent on the development of the human person (as the central subject of development as stated in the right to development Art. 2 part 1), and at that, the degree of personality development of the human person.

Heretofore, full development has been far-fetched because supposed education and development institutions or organizations, focus on the subject of development (seeking to achieve global development by focusing on developing courses and programs to resolve problems) rather than focusing on

the central subject of development (the human person-UN Right to Development –A/RES/41/128, Art. 2 Part 1); hence, the genius environment of development (full development of the human personality) is yet an imaginative experience in our world – whose unachievability is evermore promoted by concentrations on technical content and testing or exams over human-centered development, impracticable to genius development which rather requires integral development, a developmental period – organization and intelligence!!!

Clamant trainers and institutions of learning have the aforementioned as a major challenge: e.g., mental or behavioral development as part of the personal development environment required to compliment the decorum (an exclusive integral genius) of information and cybersecurity isn't considered; the ***"how"*** isn't considered – hence all methods and tools, including policies, and training institutions and or curricula, designed to mitigate cybercrime and install a global information security pathway are constantly unsustainable by reason of the aforesaid – a complete misapprehension concerning dictates to the imprimatur on education and development and cybersecurity isn't any exclusion to the rule!

Objective of Our Strategic Disposition Across Africa

Our strategy has considerably addressed the aforementioned linear development path that would deliver the most outstanding cyber practice from Africa to the rest of the world. Our goal is to metastasize a relevant and complete cyber education, via the formation of cyber teams (cyber technocrats-polymaths: 50-100-500 conditional to size of regions) across every country within the continent of Africa, apt to provide countrywide cyber awareness, education, training, and services.

The Role of Partners: Role of Partners across different African countries

As foregrounded by SDG-17, the need for a global partnership for the development of such technocratic platform for the emergence of the continent in this digital era is indisputable. Our objective in the aforesaid, is to establish effective partnerships to accomplish the vision of comprehensive (and sustainable) information security practice across the continent by the continent.

In the words of Germany's Federal Minister for Economic Cooperation and Development, Dr Gerd Müller,
"ONE WORLD – Our Responsibility." - ***Charter for the Future – forum on global partnerships, 1 April 2014, Berlin,*** **….** *One Continent, Our Responsibility*.

Dr.Coach Achu Gustave (AEC-Sr.)
CSCU, CEH, CEI
ECSD Corporate Strategist /Cyber Strategist

REFERENCES

BTH EDUCATION GROUP – ICD PROGRAM – *www.btheducationgroup.org*
ECSD TECH TRAINING PROGRAM - *https://essokacybersecuritydiv.com/our-cyber-team*
Right to Education, Article 26, part 2 – UDHR - UN
UN Right to Development, A/RES/41/128, Art. 2, part 1
Education for all – EFA UNESCO, UN - *https://en.unesco.org*
DESD – Decade of Education for Sustainable Development, UN
SDG – Sustainable Development Goals, UN
CompTIA – Computer Technology Industry Association - *https://www.comptia.org*
Cybersecurity Certifications – EC-Council - *https://www.eccouncil.org*