Online Journal of Applied Knowledge Management
A Publication of the International Institute for Applied Knowledge Management

Volume 9, Issue 2, 2021

Cybersecurity capacity building of human capital: Nations supporting nations

Michelle M. Ramim, Nova Southeastern University, USA, ramim@nova.edu

Angel Hueca, Carnegie Mellon University, USA, alhueca@cert.org

Abstract

Capacity building of human capital can be described as the experience, knowledge, skill sets, and intangible assets that add economic value to individuals and the organizations they work for. With the ever-growing gap in cybersecurity skill sets, it is essential to have a shared understanding of the necessary current skills and what those skills represent in the form of human capital to not only individuals, but also the organizations they work for. As nations around the world are struggling with the increased dependencies on Information Systems (IS) and the massive cybersecurity incidents resulting from adversaries, it is evident that cybersecurity human capital is the key in overcoming such challenges. With that said, while major players fighting cyber adversaries such as the United States (U.S.) and other western nations are struggling with their own significant cybersecurity human capital shortage, less developed nations are even further challenged. For example, African nations continue to acquire and implement ISs, the pace in which these technologies are adopted outnumbers the rate at which the skills to protect these technologies are captured. In this study we introduce the concept of cybersecurity human capital at the national level in the African region, as well as specific steps necessary to develop and embed current cybersecurity skills in cybersecurity human capital. We discuss the challenges faced by Sub-Saharan African nations in the journey to develop their cybersecurity human capital at the national level. An overview of the programs developed by the U.S. Department of State's Office of the Coordinator for Cyber Issues is provided across three case studies.

Keywords: Capacity building, cybersecurity, human capital, cyber-colonization, knowledge transfer, skills building, cybersecurity risk mitigation, Computer Security Incident Response Team (CSIRT).

Introduction

As the world's dependence on Information Systems (IS) increases, so does cybersecurity incidents and data breaches are constantly growing (Carlton et al., 2019). Cybersecurity incidents have been impacting individuals, organizations, and governments worldwide (Levy & Gafni, 2021). According to the latest 2020 annual report by the Federal Bureau of Investigation (FBI)'s Internet Crime Complaint Center (IC3) (2020), claimed that international cybercrime is on the rise associated with significant losses for over 60 countries. Cybersecurity in the context of this study is defined as:

> Computing-based discipline involving technology, people, information, and processes to enable assured operations. It involves the creation, operation, analysis, and testing of secure computer systems … including aspects of law, policy, human factors, ethics, and risk

> management in the context of adversaries, (Joint Task Force on Cybersecurity Education, 2017, p. 16).

The United States (U.S.) has recognized the importance of human capital at the national level in its fight against cyber adversaries by indicating that "Today, the U.S. government suffers from a significant shortage in its cyber workforce. Across the public sector more broadly, one in three positions (more than 33,000) remains unfilled. These shortages are driven by a need for personnel that have specific cybersecurity skills and experience" (Cyberspace Solarium Commission, 2020, p. 44). According to Carlton and Levy, (2017), cybersecurity skills were defined as "an individual's technical ability, knowledge, and experience surrounding the hardware and software required to implement IS security for mitigating a cyber-attack" (p. 18). However, while western countries are being challenged by cybercriminals, nation states, and other cyber adversaries to protect their critical infostructure, other less developed countries are even more limited in cybersecurity capabilities.

Over the past two decades Sub-Saharan Africa has experienced a dramatic surge in the implementation as well as use of Information and Communication Technologies (ICT), where, by 2011, half of the population in the region were using mobile technologies and 13% of the population were using the Internet (Wamboye et al., 2015). This technology renaissance in Sub-Saharan Africa has been so extensive that it has been named by some as "Silicon Savannah" an analogy to Silicon Valley (Park et al., 2017). This term is widely used in Nairobi, Kenya, to position the country's ICT sector as the digital technology center of Africa (Poggiali, 2016). As such, a number of governments in Africa have worked independently to introduce technology companies and innovation in their countries. Recently, cyber-colonization has been pursued by Google© in Ghana and Rwanda, as well as Facebook© in Nigeria, to name a few. These efforts are not only targeting opportunities to arrive first, however, these companies appear to also wish to influence the younger generation to use their products and services. In 2020, the United Nations (UN) estimated the total population of Africa at 1.3 billion, with 60% of the population under the age of 24 (worldmeters.info, 2020). African governments are approaching a crossroad. Not only are they working to create a stable and extensive technology infrastructure, but they also work to provide opportunities for significant training, skills acquisition for current and future African government employees, professionals, and students. The mere existence of fast Internet and foreign investments is not sufficient. Rather, the focus is on the creation of skilled cybersecurity human capital that will work with existing technologies as well as develop new innovation that will solve real life threats unique to the African continent. The need for such well trained and skilled cybersecurity human capital necessitates the formulation of cybersecurity capacity building. Thus, our aim in this paper is to further develop the concept of cybersecurity capacity building and provide case studies on how such concept was implemented in three African nations.

Background

Cybersecurity Capacity Building

In order to develop a solid definition of cybersecurity capacity building the term capacity is first defined followed by the definition for capacity building. According to Matachi (2006), capacity is defined as "the organizational and technical abilities, relationships and values that enable countries, groups and individuals at any level of society to carry out functions and achieve their development objectives over time" (p. 4). Matachi (2006) focused on three levels of capacity, namely, the environment sphere, the organization sphere and the individual sphere as illustrated in Figure 2. At each sphere a strategy is set to mobilize the particular processes and resources that are needed to enable the overall movement of knowledge and skills in a dynamic cycle of generating and building capacity. The cybersecurity capacity building framework will be introduced in the next section followed by an overview of the conceptual outlook of roles of knowledge doners on the capacity building environments, organizations, and individuals. Next, we will discuss the role of the U.S. government as a knowledge donor to support the cybersecurity capacity building in three African countries. All three knowledge donation implementations formulated around the CSIRT Development Mentoring Framework. The paper will conclude with recommendations to further enhancement build and extend the collaboration between individuals from donor nations and individuals from regions that seek to develop their cybersecurity capacity and human capital.

Capacity building denotes “the creation, expansion or upgrading of a stock of desired qualities and features called capabilities that could be continuously drawn upon over time” (Kislov et al., 2014, p. 2). Moreover, capacity building focuses on continually developing individual and organizational capabilities through knowledge acquisition and skills, as well as applying these capabilities to resolve new challenges and targets. The basis for this definition originated in the 1970s in the field of international aid for undeveloped regions. Capacity building has been used in numerous domains such as agriculture, healthcare, education, and more. In this paper, we propose the concept of cybersecurity capacity building of human capital at a regional and national levels in Africa. In this context, cybersecurity capacity building of human capital is defined as the strategic development of educating, training, and mentoring cybersecurity personnel. It is a continual learning process in which cybersecurity African personnel exercise in real life scenarios, engage in knowledge transfer, proficiency improvement, capability development, and relevant skills building across levels of complexity. According to the European Commission (2021) - International Cyber Capacity Building report, cybersecurity capacity building, also known as “Cyber Capacity Building”, is defined as the process to “develop functioning and accountable institutions that respond effectively to cybercrime and to strengthen a country’s cyber resilience” (p. 1). In many instances it involves government, trusted industry, partners, and other organizations helping each other across organizations and national borders. It started in the 1990s with the focus to fight cybercrime, and since grew to address critical national infrastructure protection, cybersecurity skills development for the workforce, disaster recovery, incident response, public awareness, and more (European Commission, 2021). Furthermore, the European Union Institute for Security Studies (EUISS) (2014) outlined specific policies, activities, and guidelines to ensure effective response to cybercrimes and to enhance cyber resilience. Another definition has been proposed by Hohmann et al. (2017) from the Global Public Policy Institute (GPPi) whereby cybersecurity capacity building is “a set of initiatives that empowers individuals, communities and governments to reap potential gains from investments in digital technologies” (p. 4). Moreover, the goal of cybersecurity capacity building is to reduce the digital divide between the cyber capabilities of countries while establishing stronger international relationships between law enforcement entities and accountable organizations to combat cybersecurity threats effectively. Based on this notation, we have created Figure 1 to illustrate the conceptual connection among the components of: capacity building, cybersecurity capacity building, and cybersecurity human capital. The focus of our work is on the innermost circle associated with the development of the cybersecurity human capital and we will provide case studies to further validate the concept.

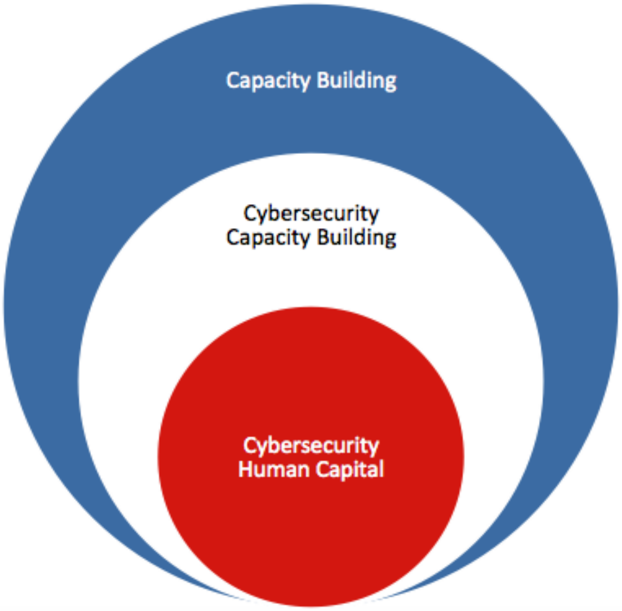


Figure 1. Conceptual Connection of Capacity Building, Cybersecurity Capacity Building, and Cybersecurity Human Capital at the national level

Cybersecurity Capacity Building Framework

Capacity building framework is associated with three levels of capacity, namely *environment, organization,* and *individual* where the environment and the organization spheres support the individual sphere, and where processes and resources at these two spheres support the knowledge and skills transfer at the individual sphere (See Table 1). Each of the three cases representing a country will outlines examples of cybersecurity processes and resources across the capacity levels by way of adapting the IICBA capacity building framework. The original IICBA Framework provided a narrow set of general elements at each level.

Table 1: Framework for Cybersecurity Capacity (Adopted from Matachi, 2006)

Level of Capacity	Cybersecurity Processes and Resources
Environment	The level of capacity referring to the *environment* represent the government of a particular country and its association to the geographical region. Processes and resources at the *environment* level include the existence of a strategy for the development of national and regional cybersecurity incident response team(s), as well as dissemination of information to members organizations in the country. In the *environment* level the government provides leadership training to member organizations either by industry types or sectors. Developing and implementing cybersecurity awareness campaigns, brochures and whitepapers to consumers, and dedicated websites for knowledge dissemination. Moreover, at the *environment* level, the government and/or region should organize events, conferences, and symposia further communicate and coordinate knowledge sharing among organizations. Furthermore, the environment level includes government(s) efforts to establish cybercrime legislation, regulation (e.g., Privacy and Data Protection Policies, Bills), and standards. Additionally, the government and/or region should establish cybersecurity educational programs

	in academic institutions, as well as promote trust and confidentiality among member organizations.
Organization	The level of capacity referring to the *organization* represent the organization and/or industry sector in a particular country. Processes and resources at the *organization* level include developing organizational contingency strategies (plan and establish teams for Incident Response (IR), Disaster Recovery (DR), and Business Continuity Plan (BCP)), facilitating technical training to individuals including leadership provided by national and international cybersecurity industry sectors experts. Additionally, the *organization* level includes coordination and facilitation of resources for meetings (e.g., yearly cybersecurity awareness campaigns, ethics training), acquired technologies to support communication and collaboration among individuals working at the organization. On the management side of the *organization* level, cybersecurity policies should be established, implemented, and audited via compliance programs. Moreover, trust and confidentiality among individuals working should promoted at the organization. Organizations should coordinate and disseminate incidents information with the environment level (i.e. regional and national) cybersecurity organizations and governmental agencies. Additionally, organization should supports developing standards for certification, and require cybersecurity professional individuals to possess educational and certifications for their job roles.
Individual	The level of capacity referring to the *individual* represent cybersecurity professional in a particular organization. Processes and resources at the *individual* level include cybersecurity knowledge and skills acquired at accredited educational and training institutions. Individual cybersecurity professionals should acquire relevant IT certifications and participating in regular knowledge and skills updates provided by the organization and/or environment. Additionally, individuals are expected to disseminate information to their workplace organization and/or environment, lead cybersecurity effort at their workplace organization and environment. It is further expected that cybersecurity professionals will promote trust and confidentiality with other individuals at their workplace organization within their sector, as well as individuals from other regional and international organizations. Participation and contribution to regional and national cybersecurity organizations is also expected from individual cybersecurity professionals (e.g., participation in working groups, committees, special interest groups, chapters of relevant cybersecurity national and international associations).

Based on the International Institute for Capacity Building in Africa (IICBA) capacity building framework, we propose the following conceptual framework illustrating the roles and relations that individual employees have across the spheres of knowledge donors (i.e. U.S., United Nations Educational, Scientific and Cultural Organization (UNESCO)), environment made up of regional alliance (i.e. A.U.) and members organizations (i.e. nations).

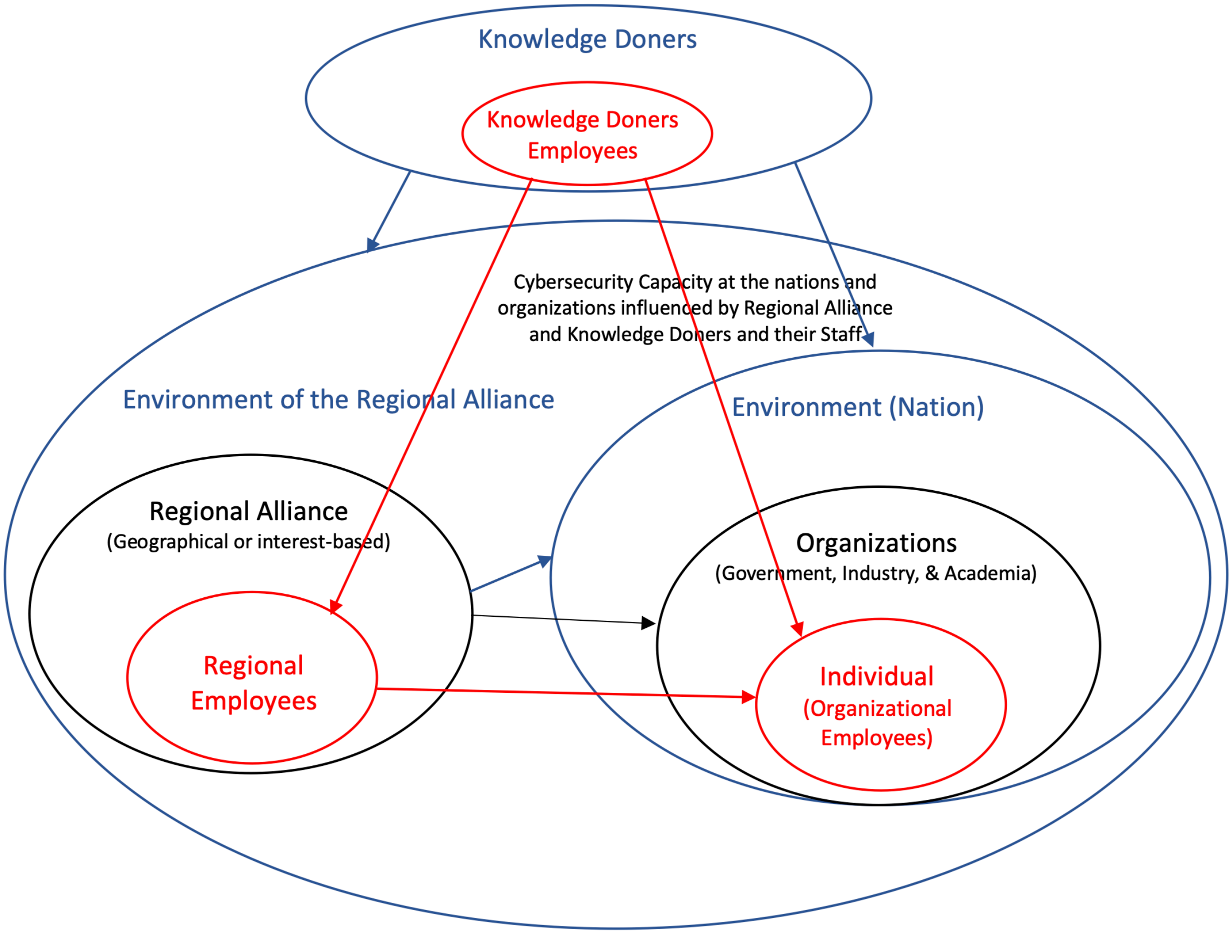

Knowledge Doners
Knowledge Doners Employees
Cybersecurity Capacity at the nations and organizations influenced by Regional Alliance and Knowledge Doners and their Staff
Environment of the Regional Alliance
Environment (Nation)
Regional Alliance
(Geographical or interest-based)
Regional Employees
Organizations
(Government, Industry, & Academia)
Individual
(Organizational Employees)

Figure 2. Conceptual Role of Knowledge Doners on the Capacity Building Environments, Organizations, and Individuals

The Cybersecurity Human Capital at the National Level

Capacity building of human capital is a critical component of cybersecurity capacity building. According to Vernizzi et al. (2016), human capital "is the set of knowledge, habits, personality attributes, competences and skills embedded in individuals and at firms' disposal" (p. 141). Additionally, human capital is needed to ensure that tasks are performed competently (Lowell, 2014). Approaches for human capital building are not new and have demonstrated to be highly successful in other fields. For example, the UNESCO and the IICBA developed a capacity building framework for building education institutions for teachers (Matachi, 2006). In the context of cybersecurity, human capital refers to combined knowledge, skills, and capabilities of the individuals, primarily the IT and cybersecurity professionals, to effectively execute tasks in mitigating cyber threats and recovering quickly from cyber incidents (Cooper et al., 2021). However, IT and cybersecurity professionals are not the only users of systems. For over a decade now, it has been well documented that the end-user is the weakest link in organizational cybersecurity (West et al., 2009). Additionally, "Many recorded industrial cyber breaches have effectively beaten technological security solutions through exploiting human-factor limitations in knowledge and skills" (Ani et al., 2019. p. 3). Beyer and Brummel (2015) stressed that when it comes to cybersecurity training, many organizations lack role-specific training, and that the emphasis is on technological countermeasures such as restricted sites and password policies, almost excluding human countermeasures like needs assessments and deception detection training. For organizational strategies protecting against cyber threats to be effective, they must include both technological and human approaches, this includes both the end-user and security/technical staff (Wright et al., 2009). Unfortunately, as the cybersecurity technological capabilities have been strengthened and further developed over the past four decades, the human capabilities are lagging behind (Carlton et al., 2018, 2019).

In most countries, it's the government that recognized early on that there is a need for a government agency or a joint-task force from different government agencies to take the lead and carry out awareness campaigns to raise public awareness for initiating cybersecurity human capital. According to Hueca et al. (2021), the primary focus of a cybersecurity awareness program "is informing users of cyber risks in an effort to influence user's behavior, and assisting the user in making the right decisions when interacting with computers and the Internet as their perform their daily responsibilities" (p. 3). National cybersecurity awareness programs include awareness-raising slogans, posters, pamphlets, etc. collaboratively with the relevant stakeholders (i.e. business organizations, academia) in the community (CISA, 2021). Other awareness activities include the creation of cybersecurity month, establishing a presence on the web and social media. Moreover, general public awareness campaigns should be created for business leaders and executives in specific industries (i.e. banking, healthcare, retail, education, etc.) in order to educate them about the cybersecurity risks and threats in their organizations (RAND Corporation, 2014). One example of a successful campaign developed by the U.S. Department of Homeland Security (DHS) is the creation of the slogan *"STOP. THINK. CONNECT.™"* that highlights to end users the risks that come with being online (CISA, 2021). This successful campaign has been extended internationally to communicate the risks associated in online activities.

An example from Africa, the country of Ghana has made a concerted effort in making cybersecurity a recognized household term. Since 2017, Ghana conducts an annual awareness campaign during October in support of "Cybersecurity Month", providing workshops for both the public and private sectors. Cybersecurity Month peaks with Cybersecurity Week, where Ghana unveils new cybersecurity services the government provides to all its constituents. The 2019 theme "Demonstrating Ghana's Cybersecurity Readiness" provided events in all regions of Ghana, as well as, several workshops and activities ranging from Child Online Protection, panel discussions, along with Cybercrime and Electronic Evidence workshops, during Ghana's Cybersecurity Week. National awareness campaigns usually stimulate organizational awareness campaigns that involve C-Level management and staff, to educate and inspire leaders to change policy and directives regarding cybersecurity. Additionally, both national and organizational awareness campaigns and training can further assist in the development of soft skills associated with cybersecurity, such as proper communication skills, due to the proper use of consistent cybersecurity terms or concepts such as phishing, vishing, social engineering, etc.

Another critical component in establishing the cybersecurity human capital involves the development of educational programs. According to Vernizzi et. al., (2016) human capital thrust in numerous intangible assets such as education, knowledge, experience, competences, and skills. Education is viewed as one of the "social mechanisms" to acquire knowledge and share it (Russ, 2021, p. 1). As knowledge half-life diminishes at a fast rate and skills become absolute, individuals are forced to engage in lifelong learning through open skills-based education. According to Russ (2021), human capital will continue to serve as an important intangible asset that will manage decisions in organizations, both corporate and government. Additionally, with the development of sophisticated systems to manage big data and Artificial Intelligence (AI) to secure the infrastructure, human capital will be essential to continue to engage in knowledge translation, verification, sharing and actionable decisions (Russ, 2021).

Leading countries around the world, along with the UN, have recognized the need for well trained and competent cybersecurity professionals to assist both companies and governments in their fight against cyber-attacks. Several countries around the world recognized it and invested significant efforts to develop their cybersecurity capacity, specifically the development of cybersecurity human capital emerging from educational institutions. For example, the US' National Security Agency (NSA) recognized as early as 1998 the need to build capacity in cybersecurity and established centers around the nation to inform, the public as well as produce highly competent professionals in cybersecurity. Moreover, the NSA launched the Centers of Academic Excellence in Information Assurance Education (CAE-IAE) program where qualified higher education academic institutions have been designated to educate, train, and qualify cybersecurity professionals for the U.S. workforce. This program was established to build the pool of qualified cybersecurity professionals in the workforce. In 2004, the DHS became a co-sponsor of the CAE-IAE program. A research designation (CAE-R) was added in 2008. In 2017, the CAE-IAE program name was changed to the CAE in Cyber Defense Education (CAE-CDE) and a designation pathway for two-year community colleges (CAE-2Y) was added. In 2019, the program added additional federal partners including the Cybersecurity and Infrastructure Security Agency (CISA), the FBI, the National Institute of Standards and Technology (NIST)/National Initiative on Cybersecurity Education (NICE), the National Science Foundation (NSF), the Department of Defense Office of the Chief Information Officer (DoD-CIO), and U.S. Cyber Command (USCYBERCOM), and was renamed to National Centers of Academic Excellence in Cybersecurity (NCAE-C) (NSA, 2022). According to the NSA (2020), when it comes to cybersecurity human capital, no single government entity or organization can develop it alone, rather it must be conceptualized as a team-sport where all 'players', government, industry, and academia must 'play together' to further develop "a future cadre of cybersecurity experts" (p. 3).

An essential component in establishing the cybersecurity human capital involves the development of human knowledge and skills. According to Russ et al. (2010), *knowledge* does not have a single ubiquitous definition. They offer a practical definition in which "knowledge is an action, or a potential of an action, that creates or has the potential to create, value based on data or previous knowledge, and/or information" (p. 2). In a 2017 report entitled "The Evolution of Security Skills" by IT certification company CompTIA, 350 organizations were surveyed in order to get an understanding of what skill sets organizations considered important on security teams. The top two cybersecurity skills identified were *infrastructure security* and *knowledge of various threats*. Both of these cybersecurity skills not only require individuals to gain an understanding of core cybersecurity concepts but must also remain current and up to date on the changing cyber landscape (CompTIA, 2017).

While awareness campaigns, educational programs, as well as knowledge and skills development in cybersecurity are important for cybersecurity human capital development, governments and organizations wishing to develop cybersecurity programs first need to identify existing assets, and infrastructure, as well as, have a clear understanding of the cybersecurity challenges they are faced by adversaries. Understanding these key components will better situate governments and organizations in determining the skills necessary for new team members, or which cybersecurity skills are needed to be enhanced in existing team members. Thus, it appears that in the focus of cybersecurity human capital development, governments and organizations must properly assess the cybersecurity skills literacy of their workforce to identify any gaps (Cyberspace Solarium Commission, 2020).

The Cybersecurity Skills Gap

Curran (2014), Cobb (2016), as well as Richardson et al. (2019) have identified in their studies, the existence of a significant cybersecurity skills gap. Subsequently, it is hampering efforts by cybersecurity professionals to defend information systems against malicious actors (Cobb, 2016). Moreover, the cybersecurity skills needed include the ability to maintain computer information systems security, protect such systems from malware, hacking, compromises, and intrusions (Vogel, 2016). Additionally, according to Nobles (2020), there is a massive global cybersecurity skills shortage, and the gap expands further as time progress due to development of new technologies. Consequently, in order to overcome the cybersecurity skills gap, the U.S. Cybersecurity National Action Plan (CNAP) (Daniel, 2016) amid at taking a lead role to "promote international cooperation, prevent attacks, and support computer emergency response teams providing reconstitution and mitigation services" (pare. 22). In support of the CNAP, the U.S. Department of State's Office of the Coordinator for Cyber Issues (S/CCI) (n.d.) has partnered with the Security Operations Team within the Computer Emergency Response Team (CERT) Division at Carnegie Mellon University (CMU)'s, Software Engineering Institute (SEI), to enhance cybersecurity capacity building with partnering nations and established the International Cybersecurity Initiatives (ICI) Team (Hueca, 2018).

Several countries in Africa have collaborated with the SEI to further develop their cybersecurity capacity. These international partnerships are important because, as noted by Elkhannoubi and Belaissaoui (2016), the developing world often lacks the controls and procedures to secure networks and systems, "making it both a target of attack, as well as a medium to attack other parts of the world" (p. 19). These vulnerabilities to cyber threats in developing countries are a direct result of the immense growth in ITC within these countries over the past decade (Jansen van Vuuren et al., 2014). Moreover, Mezzour et al. (2015), identified "that trojans, worms, and viruses, are most prevalent in Sub-Saharan Africa, mainly due to widespread computer piracy" (p. 1). These findings indicate that cybersecurity capacity building in Sub-Saharan Africa can help to further mitigate the cyber-attacks on the rest of the world.

Cybersecurity Capacity Building in Africa and U.S. Government Partnership

In the global effort to combat cybersecurity incidents, combined with the nature of the interconnectivity of governmental and organizational systems around the world, it appears important for governments with strong cybersecurity capacity to assist their allies that have very little cybersecurity capacity, especially when it comes to the cybersecurity human capacity. As such, the U.S. efforts to extend the cybersecurity capacity building in Africa have been ongoing, while serving as the knowledge donor to such African regions and countries (Bedda, 2019).

Several stumbling blocks were encountered in the early stages of the cybersecurity capacity building as many African countries even if they had financial resources, Internet infrastructure, the greatest challenge was with the lack of local cybersecurity human capital. In 2014, 54 African countries making up the African Union (A.U.) adopted the Convention on Cybersecurity and Personal Data Protection (also known as the Malabo Convention). Its three primary areas included: electronic transactions, personal data protection, as well as cybersecurity and cybercrime (African Nations, n.d.). As time progressed, only a handful of countries endorsed the convention and adopted a formal policy, resulting in a challenge for further the alliance and implementation. While some countries were very eager to start their cybersecurity capacity building efforts and ended up initiating independently, the regional cybersecurity strategy needed further support and mentorship from the knowledge donor country. In fact, under the guidance of the U.S. S/CCI, eight countries have created national cybersecurity strategies and 13 African countries have organized National CERTs (Bedda, 2019). Such initial cybersecurity digital divide had a far-reaching effect on the region's economic performance, as well as state governments and local business organizations access to cybersecurity human capital (Anye, 2021). The A.U. has long advocated the collaboration and sharing of stable technology and Internet infrastructures amongst members due to the high cost of investment, yet such an approach requires establishing trust among A.U. members. Thus, the function of the knowledge donor country played an important role (U.S. State Department, 2021a, 2021b, 2021c, n.d.).

In the U.S., several consortiums have been created to share resources, for example, the DHS's Cybersecurity Information Sharing and Collaboration Program (CISCP) enable the exchange of unclassified actionable, relevant, and timely information between stakeholders, through trusted public and private partnerships across Critical Infrastructure (CI) sectors (CISA CISCP, n.d.). The CISCP program helps stakeholders manage cyber risks through analysts-to-analyst sharing of threat and vulnerability information. Products such as Indicator Bulletins, Analysis Reports, Joint Analysis Reports, Malware Findings Reports, Malware Analysis Reports, and Joint Indicator Bulletins are shared. This information shared between CISCP stakeholders are governed using the Traffic Light Protocol (TLP) (CISA TLP, n.d.), allowing the submitter to control the handling, classification, and sharing/dissemination of their information. Another U.S. based cyber information sharing model is the Information Sharing and Analysis Center (ISAC) model. Based on a Hub-and-Spoke architecture, the central hub receives information from participating members (the spokes); the hub can either redistribute the information received to its members, or provide value added services, augmenting the data to make it more useful (MITRE, 2012).

To implement information sharing mechanisms, many African nations are following these U.S. standards. As a result, the U.S. State Department has stepped up their efforts to motivate and push a holistic government to government approach to extend the cybersecurity capacity building in the region (Curran, 2014; U.S. State Department, 2021a, 2021b, 2021c, n.d.). As noted earlier, the cybersecurity skills gap is also applicable to current employees. Often, the challenge that cybersecurity analysts have is what to do with the new tools provided (Nobles, 2020). To determine the capacity in which a Computer Security Incident Response Team (CSIRT) operates, the SEI has developed the CSIRT Development Capacity Continuum. The continuum illustrates a CSIRT's capabilities on a scale from 0, being a Nascent CSIRT, to 5, where the CSIRT is on the Leading Edge and Innovative. For a CSIRT to be classified within the continuum, a series of interviews are conducted with the partnering nations' National CSIRT. These interviews are within the scope of the SEI National CSIRT Development Mentoring Framework. This framework is applied in four linear phases as noted by Bills et al. (2016):

Phase 1: Information Discovery. This phase assists the mentor team in understanding the organization requiring mentoring and determine the feasibility for providing assistance. The information gathered here is the foundation for all the other components the framework is built on. The main activities include:

- Identify the assistance the CSIRT desires.
- Submit an information-gathering survey to the CSIRT for completion.
- Perform a public-source literature review.
- Obtain insight about the CSIRT from Post (the U.S. Embassy in the country).
- Obtain insight from partner CSIRTs.
- Interview CSIRT members.
- Conduct an onsite visit with the CSIRT.
- Obtain insights from government or industry stakeholders in the country.
- Identify previous training or mentoring received by the CSIRT.
- Perform a National CSIRT Assessment as part of the onsite visit (optional).

Phase 2: Analysis and Categorization. In this phase, data collected during the Information Discovery phase is analyzed and used to determine the current capacity of the mentee CSIRT, a plan of action is recommended in order to help improve the CSIRTs capability. The main activities include:

- Identify the CSIRT’s mission, goals, and scope.
- Identify current CSIRT activities, services, and operations.
- Identify CSIRT needs based on the assistance desired.
- Identify special circumstances.
- Benchmark the CSIRT against the CSIRT Capacity Development Continuum.
- Identify the CSIRT’s capacity level.
- Perform a gap analysis.
- Identify mentoring requirements.
- Identify potential mentors or partners.

Phase 3: Mentoring Plan Development. During this phase activities that have been jointly agreed upon by the mentor and mentee are developed and documented. This includes possible mentoring options, mentoring strategies and activities based on requirements, the creation of a corresponding roadmap along with a plan of action and milestones, as well as, socializing the plan with the mentee and its stakeholders. The main activities in this phase are:

- Identify relevant mentoring/assistance options.
- Choose mentoring strategies and activities.
- Create the mentoring plan and roadmap.
- Socialize and obtain agreement on the mentoring plan.
- Create a mentoring project plan and milestones.

Phase 4: Implementation and Evaluation. The final phase involves implementing specific mentoring tasks outlined in the mentoring and training plan, tracking the progress of the plan, and evaluating the success of the executed plan using an assessment methodology. Once the mentoring engagement is complete, the mentoring team may work with the framework maintainer to determine appropriate next steps based on lessons learned. The main activities in this phase are:

- Implement the mentoring and training plan and roadmap.
- Track milestones and accomplishments.
- Gather feedback.
- Adjust plans as needed.
- Perform a postmortem.
- Assess success.
- Gather lessons learned for inclusion in the mentoring framework.

Over the past few years, the U.S. State department has worked with several African countries to establish the cybersecurity human capital capacity building using this CSIRT Development Mentoring Framework. Furthermore, collaborative efforts are ongoing as the participating countries are continuing to work to develop advanced stages of cybersecurity human capital building, especially when it comes to the cybersecurity knowledge and skills that are evolving daily. Additionally, recently the CERT Division at CMU established a more focused framework to assist specific sectors establish their own CSIRT incident response capabilities (Novak et al., 2021).

Developing CSIRT Team Human Capital in the African Region

The CERT Division at CMU's ICI Team and U.S. S/CCI have traveled to different African nations to train officials and staff on best practices, along with how to develop their CSIRT Team and cybersecurity human capital (Hueca, 2018; Sarvepalli, 2019). "Working side-by-side with partnering governments, the [CMU's] ICI team helps identify the best path forward for cyber capacity building in line with the four strategic goals that have been outlined for national CSIRTs" (Hueca, 2018, para. 6). Below, we are listing three cases resulted from these efforts. Our sources for the tables and cases reported below are coming from open-source resources such as the Anye (2021), Hueca (2018), Hueca et al. (2021), Sarvepalli (2019), U.S. Africa Cybersecurity Group (2022), and the U.S. S/CCI's reports (2021a, 2021b, 2021c; n.d.) to name a few. To preserve the anonymity of the specific countries, we have noted the cases only with indication of the nations in a numerical form.

African Nation 1: Engagements with this nation began in 2016 and concluded in 2018. Activities included assessments of current state of CSIRT team capacity and capabilities. Direction on CSIRT maturity was provided by the knowledge donor allowing the team to instantiate proper policies and procedures. As the team evolved, they self-identified areas of needed improvement, allowing for more specific on-site training tailored to the needs of the local team in assistance, guidance, and support by the knowledge donor (See Table 2).

Table 2: Framework for Cybersecurity Capacity Framework for African Nation 1

Level of Capacity	Cybersecurity Processes and Resources
Environment	• Coordinating a national and regional cybersecurity incident response team to disseminate information to members organizations • Providing leadership training to member organizations (can be done also by industry types/sectors separately) • Coordinating and providing cybersecurity awareness campaigns • Organizing meeting to communicate and coordinate knowledge sharing efforts • Establishing standards, assessment metrics, and guidance about the legal requirements

	• Supporting cybercrime legislation and regulation • Establishing cybersecurity training programs in academic institutions • Promoting trust and confidentiality among members organizations by establishing alliances and partnerships
Organization	• Developing an organizational incident response team, facilitating technical training to individuals • Facilitating cybersecurity leadership training provided by national and international cybersecurity industry type/sectors experts • Coordinating meetings and acquiring technologies to support communication and collaboration among individuals working at the organization • Coordinating and providing cybersecurity awareness campaigns at the organization level • Developing certification and accreditation for cybersecurity professional individuals • Establishing, implementing, and assessing organizational cybersecurity policies • Promoting trust and confidentiality among individuals working at the organization • Coordinating and disseminating incidents information with regional and national cybersecurity organizations
Individual	• Cybersecurity knowledge and skills training at local educational institutions • Acquiring relevant IT certifications and participating in knowledge and skills update • Disseminating information to their workplace organization • Leading cybersecurity effort at their workplace organization • Promoting trust and confidentiality with individuals at their workplace organization in their industry/sector, as well as individuals from other regional and international organizations • Participating and contributing to regional and national cybersecurity organizations

African Nation 2: Over the course of five years between 2015 and 2020, this nation has developed a plan for an information sharing network and built up their national CSIRT capacity. To get to this point, a series of interviews and on-going conversations identified gaps in policies and procedures, conducted internally and with the knowledge donor. Once these gaps were identified, the joint team worked to create a policy and supporting process. Areas where necessary skills were missing or were scarce locally, on-site training and workshops with Subject Matter Experts (SME) were conducted in collaboration with the knowledge donor (See Table 3).

Table 3: Framework for Cybersecurity Capacity Framework for African Nation 2

Level of Capacity	Cybersecurity Processes and Resources
Environment	• Coordinating a national and regional cybersecurity incident response team to disseminate information to members organizations • Providing leadership training to member organizations (can be done also by industry types/sectors separately) • Advanced coordinaton and implementation of a cybersecurity awareness campaigns, publication of a consumer Internet Security and Privacy guide to citizens • Organizing meeting to communicate and coordinate knowledge sharing efforts via a multi-agency collaboration approach

	• Establishing standards, assessment metrics, and guidance about the legal requirements • Government established cybercrime legislation and regulation, for example, Privacy and Data Protection Policy and Bill • Government supports developing standards for certification and accreditation of cybersecurity professional individuals by adopting international standards • Advanced establishment of cybersecurity training programs in academic institutions • Promoting trust and confidentiality among members organizations by establishing alliances and partnerships with other nations in the region as well as international partners • Government established and implemented a National Public Key Infrastructure (NPKI).
Organization	• Developing an organizational incident response team, facilitating technical training to individuals in financial institutions • Facilitating cybersecurity leadership training provided by national and international cybersecurity industry type/sectors experts • Coordinating meetings and acquiring technologies to support communication and collaboration among individuals working at the organization • Strategy in place for cybersecurity awareness campaigns at the organization level at large organizations only • Establishing, implementing, and assessing organizational cybersecurity policies mostly at large organizations • Promoting trust and confidentiality among individuals working at the organization • Coordinating and disseminating incidents information with regional and national cybersecurity organizations
Individual	• Cybersecurity knowledge and skills training at local educational institutions via the government established educational network • Acquiring relevant IT certifications and participating in knowledge and skills update • Disseminating information to their workplace organization • Leading cybersecurity effort at their workplace organization • Promoting trust and confidentiality with individuals at their workplace organization in their industry/sector, as well as individuals from other regional and international organizations • Participating and contributing to regional and national cybersecurity organizations

African Nation 3: This nation had begun discussions on creating an information sharing network, to include the national CSIRT team and other stakeholders. While CSIRT teams did exist, formalization of procedures, did not. Through a series of interviews, data was collected form SMEs to create workshops tailored to the needs of all stakeholders within that nation, including specific critical infrastructure participants (See Table 4).

Table 4: Framework for Cybersecurity Capacity Framework for African Nation 3

Level of Capacity	Cybersecurity Processes and Resources
Environment	• Established a national cybersecurity incident response team to disseminate information to members organizations, as well as a cyber incident response protocol for cyber crisis • Providing leadership training to member organizations (can be done also by industry types/sectors separately) • Coordinating and providing national cybersecurity awareness campaigns "Think before you click" • Organized national cybersecurity strategy, coordination and communication of critical knowledge with organizations • Early effort of establishing standards, assessment metrics, and guidance about the legal requirements to organizations • Early effort of establishing cybercrime legislation and regulation: joined the A.U. Convention on Cybersecurity and Personal Data Protection, government approved the Computer Misuse and Cybercrime Act (CMCA) as well as aligned with the Budapest Convention on Cybercrime and African Union Convention on Cybersecurity and Personal Data Protection • Early efforts in establishing cybersecurity training programs in academic institutions • Promoting trust and confidentiality among members organizations by establishing a moderate number of alliances and partnerships between the public and private sectors
Organization	• Developing an organizational incident response team, facilitating technical training to individuals among some organizations • Some evidence of cybersecurity leadership training provided by national and international cybersecurity industry type/sectors experts • Some organizations technologies to support communication and collaboration among individuals working at the organization • Cybersecurity awareness campaigns at the organization level were needed • Establishing, implementing, and assessing organizational cybersecurity policies were needed • Promoting trust and confidentiality among individuals working at the organization • Sporadic practice of reporting incidents information to the national CERT • Developing certification and accreditation for cybersecurity professional individuals has not been achieved
Individual	• Basic cybersecurity knowledge and skills training by the national CERT • Acquiring relevant IT certifications and participating in knowledge and skills update were needed • Culture of disseminating of information at the workplace organization was needed • Participation and contribution to regional and national cybersecurity organizations were needed

African Regional Cybersecurity Capacity: U.S. collaboration with partnering nations also includes providing services for specific regions. Working with the African region, it was determined that the different national CSIRT teams from Africa were interested in creating an information sharing network (Anye, 2021; Sarvepalli, 2019; U.S. Africa Cybersecurity Group, 2022). Additionally, the U.S. continued serving as the knowledge donor by providing supporting resources including events and activities (U.S. S/CCI, 2021a, 2021b, 2021c). One such example included a workshop on best practices for information sharing to stakeholders from African nations provided by the SMEs from FIRST and the SEI (Sarvepalli, 2019). Furthermore, the aim of the U.S. support over the years was to elevate the African countries and the whole region CSIRT's capabilities on the levels of the SEI National CSIRT Development Mentoring Framework in all four linear phases (Bills et al., 2016). The investment initiated by the U.S. as the main knowledge donor, appear to impact other regions, such as the UK and other European nations, to see the value improvements have on the world's cybersecurity posture against nation states and other cyber criminals (INTERPOL, 2021).

Conclusions and Discussion

Challenges in developing human capacity and ultimately human capital at the national level are not constrained to the African region. These are human challenges that are applicable to people globally and from all walks of life. Understanding the development of human capital to meet current and future needs in the field of cybersecurity is necessary for continual online safety of individuals, organizations, and governments. Organizations must turn their attention to the cybersecurity skills and literacy of their workforce (Nobles, 2020; Russ, 2021), with a focus on specific roles within teams, and team functions within organizations, while the organizations must be synchronized with their environmental level entities as discussed above. Additionally, the cybersecurity professionals should operate within their organizational level and environment level to support the capacity building to further enhance the cybersecurity posture of their own organizations, fellow organizations within their sector, as well as their nation and region.

We see a great need for future research to focus on the intersection between culture (regional & organizational) and knowledge transfer, while assessing its impact on cybersecurity human capital building. While human capital is the knowledge, skills, and intangible assets that add economic value to individuals, it appears to be difficult to measure, especially as it is changing constantly (Calandro & Pawlak, 2014). However, measuring the value that human capital bring to governments and organizations in the form of Return on Investment (ROI) can provide a surrogate measure of human capital at the national level. Measuring ROI can be done by sampling individual or team performance over a period of time and applying metrics to determine value. One example can be cybersecurity incident detection; how many incidents are correctly identified at the beginning of said time frame, versus, how many cybersecurity incidents were correctly identified after training, over a period of time. The metric lies not only in correct incident classification, but how much money the organization or a nation saved, due to improved overall organizational productivity, because of correct incident classification and eradication, reducing the window of downtime, where employees could not work. Thus, we recommend that future research should also focus on the assessments of ROIs when it comes to implementations of National CSIRT teams and further enhance their cybersecurity capacity and human capital.

Acknowledgement

We would like to thank the U.S. State Department Office of the Coordinator for Cyber Issues, and the CERT Division at the Software Engineering Institute, Carnegie Mellon University, for their ongoing work in securing cyberspace for all nations. Additionally, we would like to thank Professor Meir Russ for his outstanding feedback, comments, and numerous valuable recommendations that helped improve this manuscript.

References

African Union, (n.d.). Retrieved from https://ccdcoe.org/organisations/au/

Ani, U. D., He, H., & Tiwari, A. (2019). Human factor security: Evaluating the cybersecurity capacity of the industrial workforce. *Journal of Systems and Information Technology, 21*(1), 2-35. https://doi.org/10.1108/JSIT-02-2018-0028

Anye, D. S. (2021). *Top digital transformation and innovation countries in Africa: A comprehensive comparison of technology development in the African continent*. Independently published.

Bedda, C. (2019). https://au.int/en/speeches/20180723/speech-auc-director-infrastructure-energy-workshop-cyber-strategies-cyber

Beyer, R. E., & Brummel, B. (2015). Implementing effective cyber security training for end users of computer networks. *Society for Human Resource Management and Society for Industrial and Organizational Psychology*. https://www.shrm.org/hr-today/trends-and-forecasting/special-reports-and-expert-views/Documents/SHRM-SIOP%20Role%20of%20Human%20Resources%20in%20Cyber%20Security.pdf

Bills, T., Lord, J., McIntire, D., Ruefle, R., & Zajicek, M. (2016). *National computer security incident response team development mentoring framework* (pp. 1–88). Carnegie Mellon University.

Calandro, E., & Pawlak, P. (2014). Capacity building as a means to counter 'cyber poverty'. In Pawlak, P. (Ed.), *Riding the digital wave: The impact of cyber capacity building on human development* (pp. 52-60). https://www.iss.europa.eu/sites/default/files/EUISSFiles/Report_21_Cyber.pdf

Carlton, M., & Levy, Y. (2017). Cybersecurity skills: The cornerstone of advanced persistent threats (APTs) mitigation. *Online Journal of Applied Knowledge Management, 5*(2), 16-28. https://doi.org/10.36965/OJAKM.2017.5(2)16-28

Carlton, M., Levy, Y., & Ramim, M. M. (2018). Validation of a vignettes-based, hands-on cybersecurity threats situational assessment tool. *Online Journal of Applied Knowledge Management, 6*(1), 107-118. https://doi.org/10.36965/OJAKM.2018.6(1)107-118

Carlton, M., Levy, Y., & Ramim, M. M. (2019). Mitigating cyber attacks through the measurement of non-IT professionals' cybersecurity skills. *Information and Computer Security, 27*(1), 101-121. https://doi.org/10.1108/ICS-11-2016-0088

Cobb, S. (2016). Mind this gap: Criminal hacking and the global cybersecurity skills shortage, a critical analysis, (October), 1–8. Retrieved from: https://www.virusbulletin.com/uploads/pdf/magazine/2016/VB2016-Cobb.pdf

Cooper, M., Levy, Y., Wang, L., & Dringus, L. (2021). Heads-up! An alert and warning system for phishing emails. *Organizational Cybersecurity Journal: Practice, Process and People, 1*(1), 1-22. https://doi.org/10.1108/OCJ-03-2021-0006

CompTIA. (2017). *The evolution of security skills*. *Research Report*. https://connect.comptia.org/content/research/the-evolution-of-security-skills

Curran, J. (2014). *Cybersecurity policy report.* New York.

Cybersecurity and Infrastructure Security Agency (CISA) (2021). *CISA cybersecurity awareness program.* https://www.cisa.gov/cisa-cybersecurity-awareness-program

Cybersecurity and Infrastructure Security Agency (CISA) (n.d.). *Cybersecurity Information Sharing and Collaboration Program (CISCP). https://www.cisa.gov/ciscp*

Cybersecurity and Infrastructure Security Agency (CISA) (n.d.). *Traffic light protocol (TLP) definitions and usage*. https://www.cisa.gov/tlp

Cyberspace Solarium Commission (2020). Report. https://www.solarium.gov/report

Daniel, M. (2016). The president's national cybersecurity plan: What you need to know? https://obamawhitehouse.archives.gov/blog/2016/02/09/presidents-national-cybersecurity-plan-what-you-need-know

Elkhannoubi, H., & Belaissaoui, M. (2016). Assess developing countries' cybersecurity capabilities through a social influence strategy. *Proceedings of the 7th International Conference on Sciences of Electronics, Technologies of Information and Telecommunications*, pp. 19-23. https://doi.org/10.1109/SETIT.2016.7939834

European Commission (2021). International cyber capacity building report. https://www.iss.europa.eu/sites/default/files/EUISSFiles/CCB%20Report%20Final.pdf

European Union Institute for Security Studies (EUISS) (2014). *Cyber capacity building in ten points' note based on deliberations during the international conference on cyber capacity building*. EU Institute for Security Studies, Paris.

Federal Bureau of Investigation (2020). *2020 Internet crime report.* Internet Crime Complaint Center (IC3). https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf

Forum of Incident Response and Security Teams (FIRST) (2021). *CSIRT Framework.* https://www.first.org/standards/frameworks/csirts/

Hohmann, M., Pirang, A., & Benner, T. (2017). *Global public policy institute*. Retrieved from: http://www.gppi.net/publications/data-technology-politics/article/advancing-cybersecurity-capacity-buildingimplementing-a-principle-based-approach/

Hueca, A. L. (2018). *Engaging the CSIRT community cyber capacity building on a global scale. https://insights.sei.cmu.edu/blog/engaging-the-csirt-community-cyber-capacity-building-on-a-global-scale/*

Hueca, A. L., Manley, B., & Rogers, L. (2021). *Building a cybersecurity awareness program*. Carnegie Mellon University, Software Engineering Institute (SEI), CERT Division Handbook. https://resources.sei.cmu.edu/asset_files/Handbook/2021_002_001_651800.pdf

INTERPOL (2021, May 12). *INTERPOL launches initiative to fight cybercrime in Africa.* https://www.interpol.int/en/News-and-Events/News/2021/INTERPOL-launches-initiative-to-fight-cybercrime-in-Africa

Jansen van Vuuren, J. C., Leenen, L., & Zaaiman, J. (2014). Using an Ontology as a Model for the Implementation of the National Cybersecurity Policy Framework for South Africa. *Proceedings of the 9th International Conference on Cyber Warfare & Security*, pp. 105-115.

Joint Task Force on Cybersecurity Education (2017). Curriculum guidelines for post-secondary degree programs in cybersecurity. https://cybered.hosting.acm.org/wp-content/uploads/2018/02/newcover_csec2017.pdf

Kislov, R., Waterman, H., Harvey, G., & Boaden, R. (2014). Rethinking capacity building for knowledge mobilisation: Developing multilevel capabilities in healthcare organisations. *Implementation Science, 9*(166).

Levy, Y., & Gafni, R. (2021). Introducing the concept of cybersecurity footprint. *Information and Computer Security*. https://doi.org/10.1108/ICS-04-2020-0054

Lowell, L. (2014). Human capital capacity building; The essence of organizational development. *International Journal of Science and Research, 3*(12), 2174-2175.

Matachi, A. (2004). *Capacity building framework.* UNESCO – International Institute for Capacity Building in Africa. https://unesdoc.unesco.org/ark:/48223/pf0000151179

Mezzour, G., Carley, K. M., & Carley, L. R. (2015). An empirical study of global malware encounters. *Proceedings of the 2015 Symposium and Bootcamp on the Science of Security*, 1-11. https://doi.org/10.1145/2746194.2746202

MITRE. (2012). *Cyber information-sharing models: An overview*. McLean. Retrieved from: http://www.mitre.org/sites/default/files/pdf/cyber_info_sharing.pdf

National Security Agency (2020). *National centers of academic excellence in cybersecurity journal (2020 Edition).* https://www.caecommunity.org/sites/default/files/CAE_Book_Version_2.0_Compressed.pdf

National Security Agency (2022). *The National Centers of Academic Excellence in Cybersecurity (NCAE-C) program.* https://www.nsa.gov/Academics/Centers-of-Academic-Excellence/

Novak, J., Manley, B., McIntire, D., Mudd, S., Hueca, A. L., & Bills, T. (2021). *The sector CSIRT framework: Developing sector-based incident response capabilities*. Carnegie Mellon University, Software Engineering Institute (SEI), CERT Division Technical Report. https://resources.sei.cmu.edu/asset_files/TechnicalReport/2021_005_001_734796.pdf

Nobles, C. (2020). The cyber talent gap and cybersecurity professionalizing. In Burrell, D. N. (Ed.), *An Exploration of the Cybersecurity Workforce Shortage (pp. 56-63).* IGI Global. https://doi.org/10.4018/978-1-7998-2466-4.ch063

Park, E. K., Martins, R. M., Hain, D., & Jurowetzki, R. (2017). Entrepreneurial ecosystem for technology start-ups in Nairobi: Empirical analysis of twitter networks of start-ups and support organizations. In *Danish Research Unit for Industrial Dynamics* (p. 35).

Poggiali, L. (2016). Seeing (from) digital peripheries: Technology and transparency in Kenya's Silicon Savannah. *Cultural Anthropology*, *31*(3), 387–411. https://doi.org/10.14506/ca31.3.07

RAND Corporation (2014). *Homeland security: October is the cybersecurity awareness month.* https://www.rand.org/congress/alerts/2014/october-is-cybersecurity-awareness-month.html

Richardson, L. C., Lewis, S. M., & Burnette, R. M. (2019). *Building capacity for cyberbiosecurity training, 7.*

Russ, M. (2021). Knowledge management for sustainable development in the era of continuously accelerating technological revolutions: A framework and models. *Sustainability, 13,* 3353. https://doi.org/10.3390/su13063353

Russ, M., Fineman, R., & Jones, J. K. (2010). Conceptual theory: What do you know? In M. Russ (Ed.), *Knowledge Management Strategies for Business Development* (pp. 1-22). IGI Global. https://doi.org/10.4018/978-1-60566-348-7.ch001

Sarvepalli, V. (2019). *Securely connecting Africa*. https://insights.sei.cmu.edu/blog/securely-connecting-africa/

U.S. Africa Cybersecurity Group (2022). https://www.usafcg.com/

U.S. Department of State (n.d.). *Office of the Coordinator for Cyber Issues (S/CCI).* https://www.state.gov/bureaus-offices/secretary-of-state/office-of-the-coordinator-for-cyber-issues/

U.S. Department of State (2021, December 2). *Modernizing cybersecurity in U.S. diplomatic technology: Our global call to action.* https://www.state.gov/modernizing-cybersecurity-in-u-s-diplomatic-technology-our-global-call-to-action/

U.S. Department of State (2021, December 3). *United States and Kenya hold dialogue on cyber issues.* https://www.state.gov/united-states-and-kenya-hold-dialogue-on-cyber-issues/

U.S. Department of State (2021, December 11). *U.S. diplomats build cyber defense and cybersecurity partnerships worldwide.* https://www.state.gov/u-s-diplomats-build-cyber-defense-and-cybersecurity-partnerships-worldwide/

Vernizzi, S., Zanoni, A. B., & Russ, M. (2016). Strategic inertia vs. strategic change: The role of human capital in fiat's turnaround pathway. In M. Russ (Ed.), *Quantitative Multidisciplinary Approaches in Human Capital and Asset Management* (pp. 123-141). IGI Global. https://doi.org/10.4018/978-1-4666-9652-5.ch007

Vogel, R. (2016). Closing the cybersecurity skills gap. *Salus Journal*, *4*(2), 32–46.

Wamboye, E., Tochkov, K., & Sergi, B. S. (2015). Technology adoption and growth in sub-Saharan African countries. *Comparative Economic Studies*, *57*(1), 136–167.

West, R., Mayhorn, C., Hardee, J., & Mendel, J. (2009). The weakest link: A psychological perspective on why users make poor security decisions. Social and Human Elements of

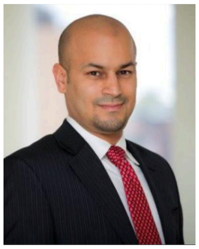
Information Security: Emerging Trends and Countermeasures, 43-60. https://doi.org/10.4018/978-1-60566-036-3.ch004

World Population (2020). https://worldmeters.info/

Wright, R., Chakraborty, S., Basoglu, A., & Marett, K. (2009). Where did they go right? Understanding the deception in phishing communications. *Group Decision and Negotiation, 19*(4), 391–416.

Authors' Biographies

Michelle M. Ramim, Ph.D., MBA is the interim director of the Bachelor of Science in Health Informatics program as well as an Assistant Professor, at Nova Southeastern University, Dr. Kiran C. Patel College of Osteopathic Medicine, Department of Health Informatics. She has over 30 years' experience in the healthcare field and extensive experience as an Information Technology (IT) consultant for small and mid-size organizations. She has directed the development and implementations of several IT projects in the healthcare field and held a license as well as practiced in the 1990s as an Assisted Living Facility Administrator. Her current research interests include healthcare IT, security of wearable and implantable devices, cybersecurity, risk management, as well as ethical and legal aspects of computing. She has published articles in peer-reviewed outlets including journals, conference proceedings, encyclopedias, and an invited chapter. Moreover, she has been serving as a referee research reviewer for national and international scientific journals, conference proceedings, as well as MIS textbooks. She completed her Ph.D. in Information Systems at the formerly known Graduate School of Computer and Information Sciences, Nova Southeastern University in the area of ethical decision making in computing.



Angel Luis Hueca, Ph.D. is a Senior Cybersecurity Operations Researcher at the CERT® Coordination Center of Carnegie Mellon University's Software Engineering Institute (SEI). He has over 20 years of combined experience in Systems Administration and Cybersecurity. Angel has worked extensively in the private and public sector implementing intrusion detection systems (IDS) and systems auditing solutions. Currently, his focus is on international CSIRT initiatives. His previous professional experience includes being the Cybersecurity Program Information Systems Security Officer (contractor) at the Consumer Financial Protection Bureau (CFPB), where he served as the bureau Cyber Policy Manager and CyberPMO Plan of Actions and Milestones (POAM) manager for the CFPB cybersecurity program. Prior to that, Angel worked at the IRS as a Senior Cybersecurity Associate (contractor) and the Pension Benefits Guaranty Corporation (PBGC) as an Information Systems Security Engineer (contractor). Additionally, Angel worked at the Independent Community Bankers of America (ICBA) and TCM Bank as the IT Operations Manager and Senior Systems Administrator, introducing formal cybersecurity practices. Angel holds a dual MS/MBA in Cybersecurity and a Ph.D. in Information Systems, focusing on information security and insider threat.