جامعة نايف العربية للعلوم الأمنية
NAIF ARAB UNIVERSITY FOR SECURITY SCIENCES
تأسست ١٩٧٨ Est. 1978

Naif Arab University for Security Sciences
Journal of Information Security and Cybercrimes Research
مجلة بحوث أمن المعلومات والجرائم السيبرانية
https://journals.nauss.edu.sa/index.php/JISCR

JISCR

Social Work in Cybersecurity: Insight Into Human Factors

Samah Monammed Albargi

Department of Social Work, Umm Al-Qura University, Saudi Arabia

CrossMark

Received 22 Oct. 2024; Accepted 07 Dec. 2024; Available Online 31 Dec. 2024

Abstract

The modern cyberspace features complex and highly evolving threats against users and particular vulnerable groups, such as youths and children. Rather than being a purely technical domain, cyber-security is a complex and multi-dimensional field that requires comprehensive evaluations and understanding of human behavior, social dynamics, and prevailing organizational structures, especially considering the increasingly sophisticated nature of cybercrimes in today's society. To be effective, cyber-security requires critical considerations of current and evolving human factors and processes, including the complex processes of interactions between technology and human belief-thought-behavior patterns, in protection, detection, response, and recovery programs. This study applies a review and synthesis of relevant findings in a sample of 25 credible sources to demonstrate and prove the critical and special value and place of social work, as a field, in cyber-security and its goals. Findings in the review show that social work has special value in effective cyber-security programs, based on its unique capacity to mobilize useful societal and human knowledge and resources to confront and address the complex and evolving nature of cyber-threats from a holistic approach. This value rests on social work's foundations and fields of practice, particularly the person-in-environment and human behavior in a social environment (HBSE) models, social work policy practice, forensic and clinical social work, and community development. Collaborations between social work and information/computing sciences based on these foundations/fields of social work represent an important pathway toward more productive, sustainable, impactful, and socially just cyber-security programs in the modern society.

I. Introduction

"The idea that cyber-security starts and ends with the purchase of a pre-packaged firewall is simply misguided." "Effective cyber-security is not a product or a set of products, but a process."These quotes from Brainyard editor Art Wittman and American politician James Langevin illustrate the complex nature of cyber-security initiatives and programs. Rather than being a one-time event or a definite structure of particular goals and end products, cyber-security is a continuous cycle of efforts and improvements targeting protection, detection, response, and recovery [1]. Ultimately, as experience over time illustrates, effective cyber-security involves complex, continuing, and evolving sets of products, practices, and interventions aimed at protecting not only information systems and devices but also the individuals and communities who access and utilize these systems.

Keywords: cybersecurity, human behavior, information security, layers of cyberspace, psychological and environmental factors, social work

Production and hosting by NAUSS

* Corresponding Author: Samah Monammed Albargi
Email: drsamahalbargi@gmail.com

doi: 10.26735/YZOF9073

A critical implication of this assessment is the need to adopt a holistic and proactive approach to cyber-security to protect information systems and people/communities. As observed in [2], social work is a potentially valuable field and pathway in the aims of cyber-security programs and interventions to empower individuals and communities to protect themselves. This value of social work is significant due to its emphasis on advocacy, change and development, social cohesion, the empowerment and liberation of people, and the principles of social justice, human rights, and collective responsibility to enhance individual and collective well-being.

II. Related Work Materials

A. Problem Statement

Cyber-crimes and threats represent one of the most prominent problems in today's society. These crimes and threats have evolved in scope and scale over time, especially with improving technologies and innovation, making it increasingly hard for governments, security agencies, and society members to protect themselves and their systems from attacks and the perpetrators' ill motives. In the face of these threats, more proactive and effective ways of protecting cyber-infrastructure, systems, and users should be identified.

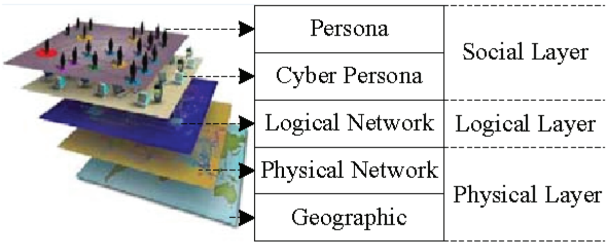

Fig. 1. Illustration of the three layers of cyberspace

Human factors represent a critical element of modern cyber-threats. As noted in [3], human factors, particularly human choices, beliefs, motivations, and behaviors, are an important area of focus in cyber-security efforts and interventions. The human element of cyberspace is integral to proactive and effective efforts in cyber-security because cyber-crime and threats target and harness human behaviors, roles, behaviors, and interactions within the cyber-space to achieve their ends. The rise of social engineering, whereby, as observed in [4], [5], and [6], human choices, behaviors, and interactions complement technical attacks in cyber-space, exemplifies this central role of human factors in cyber-security. At the same time, the primary victims of cyber-threats and crimes are human beings, communities, and societies, through financial, safety/security, well-being, infrastructural damages and losses in their lives and environments. In effect, proactive, competent, and sustainable cyber-security programs and interventions in today's world should effectively harness and integrate the human element of cyber-space in cyber-security programs. The focus of social work on understanding human beings' problems in the context of their environments, including at the personal, community, and sociocultural levels, promises potentially huge value in efforts to integrate and harness the human element of cyber-space in proactive and effective cyber-security interventions. In this context, it is essential to explore the potential value of this field in the structuring, development, and implementation of cyber-security programs to effectively and proactively combat modern cyber-crimes and threats.

The aim of this study is to show and prove the critical and special value and role of social work as a field in cyber-security and its goals. In particular, the study aims to prove that social work can help enhance cyber-security by integrating important insight into relevant human, psychological, sociological, and environmental factors and experiences in software building and applications, policy-making, protection systems, community development programs, and the empowerment of individuals and communities against cyber-threats/crimes. To achieve this goal, the paper explores the value of social work in enhancing cyber-security interventions based on the three layers of the cyber-space: physical, logical, and social/cyber-persona

The cyber-persona/social layer consists of the human elements of cyberspace. These elements comprise user identities and human interactions, roles, and behaviors within this space [3] [7]. The physical layer includes tangible network and geographical components of cyberspace infrastructure, such as servers, networking equipment, data centers, and physical connections, which form the foundation on which the cyber-persona and logical layers operate [3] [7]. The logical layer encompasses protocols, software, and configurations (such as operating systems, firewalls, applications, and encryption systems) that run/control the operations of cyberspace infrastructure [3]. As observed in [3] and [7], cyber-security issues involve complex interactions among the three layers of cyber-space. This study explores the role and impact of social work in enhancing cyber-security by providing and integrating insight into the interactions of human, psychological, sociological, and environmental factors across the three layers of cyberspace in policy-making, advocacy, protection, and community-development interventions/programs

III. Methodology

The study adopts the approach of a review or synthesis relevant findings in published literature to achieve its goal. A total of 25 articles from relevant journals and online sources were chosen for the review based on the CRAAP (currency, relevance, authority, accuracy, and purpose) criteria for resource/information credibility. The “currency” criterion required selected resources and information in them to be up-to-date (not outdated), and the “relevance” criterion demanded the inclusion of resources with appropriate content for the topic of social work and its potential value in cyber-security. The “authority” criterion required the chosen resources to be authoritative on this topic, in terms of their authors’ qualifications, experience, and expertise or the credibility of journal/website sources. The “accuracy” criterion required the selected articles to be reliable and truthful, such as in terms of being evidence-based. The “purpose” criterion required the chosen resources to be free of biases or conflicts of interest. Together, these criteria ensured the credibility of used resources. The study focused on analyzing and organizing findings in the 25 chosen articles into salient themes (patterns of ideas) in accordance with the aim to evaluate and demonstrate the critical and special value of the social work field in cyber-security and its goals.

IV. Literature Review/Results

A. Special Role/Position of Social Work in Cyber-Security

One important finding in published literature concerns the existence of a close relationship between cyber-security and social and human sciences. As observed in [7], human and social sciences have shown consistent interest in cyber-security since the latter’s emergence in security debates in the early 2000s. Published literature recognizes that national security, including cyber-security, requires investment in social cyber-security with regard to complex and evolving human interactions between technology and social beliefs and behavior [3]. Risks and threats from the cyberspace affect national security and public safety directly owing to the deep penetration and widespread use or applications of, and reliance on, computer and information systems in the society [7]. Published literature acknowledges further that rather than being a purely technical domain, cyber-security is a complex and multi-dimensional field that necessitates comprehensive evaluations and understanding of human behavior, social dynamics, and prevailing organizational structures, especially with the increasingly sophisticated nature of cybercrimes in today’s society. In this context, social and human sciences are essential to mobilize and provide useful knowledge and resources, such as social awareness, insight into human factors and user behavior, knowledge of ethical and privacy issues, political will, legislative changes, policy-making, and mental representations, in cyber-security [8]. Cyber-security experts and governments worldwide increasingly recognize a need to adopt more proactive and holistic approaches, particularly from social and cognitive perspectives, to information/cyber defenses and protection [7]. These findings demonstrate significant and longstanding recognition of a close relationship between cyber-security and social and human sciences in published literature. The basis of this recognition is traditional and doctrinal (belief-related) understanding of the cyberspace as including the physical, logical, and cyber-persona layers, such that effective cyber-security should embrace all three layers [3] [7]. As these findings illustrate, the society recognizes a need to integrate human and social sciences with information, security, and computing sciences to confront and address information risks and threats effectively in the 21st Century.

While the close and long-standing relationship between cyber-security and social and human sciences is clear in published literature, it is essential to understand the particularly critical and special role and value of social work, as a field, in cyber-security. As established in [4], social work is a practice-based profession with a key duty to promote development through positive social change and the empowerment of individuals and communities to confront and solve their problems. This profession aims to promote human and community well-being based on the principles of scientific inquiry and knowledge, a person-in-environment framework, a global perspective, and respect for human diversity; all these principles support a quest for socioeconomic justice and efforts to alleviate threats to human rights, prosperity, safety, and holistic wellbeing [4]. Fig.2 below represents the person-in-environment model, which is an important foundation of social work practice [17]. This model holds that diverse factors in people's environments, including at the personal and socio-cultural levels, have an important influence on their choices, behaviors, safety, and well-being [17].This model forms an important foundation of social work practice [17]. The person-in-environment approach in social work has special value in cyber-security because it recognizes the role of factors in the lives and environments of individuals in their decisions, behaviors, safety, and well-being. As [2] observe, adopting a societal security-based approach to cyber-theory/policy/action is increasingly essential to confront and address cyber threats effectively and proactively. Effective cyber-security requires critical considerations of current and evolving human factors and processes, including the complex processes of interactions between technology and human belief-thought-behavior patterns, in protection, detection, response, and recovery programs [7]. The special value of the social work field lies in its unique capacity to mobilize useful societal and human knowledge and resources to confront and address the complex and evolving nature of cyber-threats from a holistic approach, thus promoting the competent empowerment of organizations, communities, and individuals against these threats.

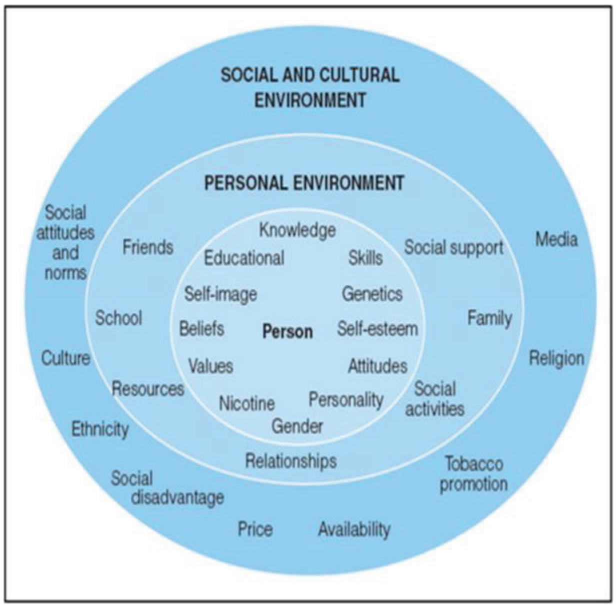

Fig. 2. A representation of the person-in-environment model

Social work is an especially valuable field in cyber-security because of the critical role of societal factors in cyber-threats today. As [2] observe, security threats today are increasingly and mostly about the ways in which human collectivities (groups) relate with one another, especially based on their social and collective identities. These identities are often factors of the interrelationship between state and society, but they could also operate independently of the state. They also evolve over time subject to both internal and external factors in the daily experiences of individuals and groups, including fears of losing own identity and global issues such as migration [2]. In this context, as [2] observe, cyber-attacks are often the outcome of social and political tensions between identity groups or strategic aims to exacerbate these tensions. In essence, socio-psychological dynamics are important underlying causes of cyber-security risks and threats in the modern society [3]. In this context, social work's emphasis on a person-in-environment approach to the experiences and problems of individuals and communities is an important empowerment and problem-solving model in cyber-security programs. This approach is essential to enable holistic assessments of the environments and experiences of individuals and communities, and guide competent policies, software development and applications, and protection, defense, empowerment, and community development programs for optimum and sustainable cyber-security.

B. Social work and Computer/Information Security Sciences

Psychological and environmental factors play a critical role in impacting human behavior. As established in [8] and [9], theories such as those of social cognition, planned behavior, and social learning reflect the processes of people's learning and development of behavior based on the interactions that they have with their environments. In particular, this development and learning occurs through modelling – as individuals observe and imitate others and utilize their cognitive resources to evaluate the consequences of behavior and adapt their behaviors to their needs and preferences. Social theories further highlight the critical roles of people's environments and interactions with these environments in shaping their motivations, performances, goals or aspirations, skills, identities, and the ways in which they self-regulate [8]. These influences also promote development or changes in human beings' personalities [9] [10]. The critical role of psychological and environmental factors in human behavior is also evident in the theory of constructivism. As established in [9] and [10], constructivism insists on the social embeddedness of knowledge and learning, suggesting that individuals are active agents who develop knowledge and meanings from the experiences that they have in their environments. As noted further in [11] [12] [13], individuals' attitudes, and available information and subjective norms in their environments, are outcomes of the beliefs that they form out of knowledge and experiences in their social environments. In essence, these findings in literature indicate the critical role of the psychological and environmental experiences of individuals in shaping their choices, knowledge, and behavior. The social environments of people involve complex, two-way processes in which individuals influence others and their choices, identities, goals, and behaviors, and others, in turn, influence them. These theories indicate the critical influences of social and environment-level factors and processes in the behaviors that individuals adopt, and the ways in which these behaviors develop or change over time. They show that it is impossible to separate human behavior from prevailing environmental and sociocultural factors and experiences in the lives of individuals.

Competent assessments of relevant social and environmental factors are increasingly essential to strengthen cyber-security. Effective and proactive cyber-security initiatives, especially those aimed at protecting individuals and communities (rather than the systems themselves alone) require in-depth understanding of the "digital playground" and the ways in which individuals who are socially and digitally embedded could experience manipulation in this space [8]. This need has led to the emergence of a new scientific and engineering discipline: social cyber-security [11]. As established in [11], social media engagements are important influences on people's beliefs, opinions, and attitudes in today's high-tech world. The modern cyber-space features consistent trends of diverse actors influencing and disrupting civil discourse, creating discord and spreading misinformation. Additionally, it features the use of diverse technologies, including bots, sock-puppets, deep fakes, cyborgs, trolls, and memes, to challenge the civil society and advance business and antagonistic agendas [14]. As established in [3], [11], [12], and [15], the field of social cyber-security has emerged in response to these threats. It is an applied computational social science with two critical objectives. The first objective is to characterize, understand, and anticipate/forecast cyber-mediated changes in human behavior and in sociocultural and political outcomes [11] [12]. Secondly, social cyber-security focuses on building or designing a social cyber infrastructure to allow the society's essential character to persist and thrive in a cyber-mediated information environment characterized by changing conditions, actual and possible social cyber-threats, and cyber-mediated threats [11]. These factors indicate a critical need to identify, understand, counter, and evaluate or measure the mechanisms and impact of communication objectives and influence campaigns, as well as identify and protect people and communities at risk from these campaigns [11]. As established in [16], cyber-security programs in recent years have incorporated proactive measures targeting social and environmental factors in the lives and cyber-use experiences of people, such as continuous education and specialized and individualized support services, to combat pig butchering scams (scams involving exploitation of social engineering to build trust and execute financial fraud). These issues indicate the critical value of efforts to understand, evaluate, and counter relevant psychological and environmental factors and experiences in the cyber-space with important underlying roles and impact in cyber-security.

Social work enhances cyber-security by facilitating the incorporation of competent knowledge of the psychological and environmental factors and processes of human behavior in cyber-security interventions and programs. As established in [3], effective cyber-security, especially in the modern age of complex and constantly evolving threats, requires competent understanding of the ways in which human beings and communities navigate the cyber-mediated information space and interact and engage in activities and conversations with others. Social work, as a field, provides a key pathway to achieve this goal. Its focus on person-in-environment, holistic assessments of the needs, problems, and experiences of individuals and communities enhances cyber-security by enabling competent simulation of the minds, motivations, experiences, and behaviors of cyber-criminals and making it easier for cyber-security experts and programs to detect, prevent, track, and counter the activities of these criminals electronically.

The value of social work is especially notable with the rise of social engineering. As observed in [4], [5], and [6], social engineering is a non-technical form of attack based on human interactions to complement technical attacks in cyber-space. It encompasses the application of social disguises, cultural tricks, and psychological/emotional manipulation to get computer users (the targets/victims) to assist cyber-criminals in their unlawful intrusion and use of computer systems/networks. Social engineering is especially significant because of its legitimate and harmless appearance, such that cyber targets are often unaware of being victimized [17]. As established in [4] and [5], rising recognition that professional cyber-criminals attack human beings, rather than machines themselves, indicates that human beings represent a critical weak link in modern information security and cyber-security incidents, with their behaviors being an important cause and perpetrating factor in cyber-security incidents. Social work is essential to provide critical factual insights into the machinations or schemes of cyber-criminals to allow computer and information sciences to predict and counter cybercrimes. In this way, social work completes the effectiveness and productivity of cyber-security programs and initiatives by providing a critical capacity to simulate and anticipate the minds, motivations, goals, and behaviors of criminals in the cyberspace.

C. Social Work Policy Practice

Social work practice presents further critical value in the development and improvement of policies and laws aimed at protecting and empowering individuals and vulnerable communities, such as children, from cybercrimes. Social work practice emphasizes on key values with important impact on the development and improvement of these laws and policies. These values are scientific knowledge and investigation, the person-in-environment framework, a global perspective, and acknowledgement and respect for human diversity [14]. As established in [8], these values are essential to support positive social change and the empowerment of individuals and communities to confront and solve their problems, based on individualized interventions that integrate considerations of their unique experiences, needs, and environments. Social work practice embraces the critical principles of the "human behavior in a social environment" (HBSE) concept [14]. This concept seeks an understanding of human behavior, including all the attributes and contributing factors of this behavior, the social environment, varying levels and systems of the social environment, and the interface between human behavior and the social environment [14]. This concept fits in with the person-in-environment model in social work, which focuses on in-depth understanding of the impact of human environments and all their features, processes, and experiences, on human wellbeing and development from a holistic perspective [4]. The critical implication of the person-in-environment and HBSE frameworks is that social work, as a discipline and practice, considers both individuals and the multiple environments and environmental factors with which they interact, based on an acknowledgement of the reciprocal relationship between them. This focus in social work is essential to support policies, interventions, and programs aimed at positive social change and the empowerment of individuals and communities to confront and solve their problems. As established in [18], the person-in-environment and HBSE frameworks are important foundations of the meaningfulness and impact of social work practice, especially with regard to facilitating a comprehensive understanding of the needs and experiences of individuals. In particular, these frameworks enable social work practice to obtain key and in-depth insight into the environmental, sociopolitical, psychological, and other factors and influences with critical role in the health and wellbeing of individuals and local communities.

The focus of social work practice on holistic and in-depth assessments of persons/communities and their environments and needs offers huge value in the efforts of cyber-security interventions to develop and enforce competent laws and policies to protect and empower individuals and communities against cybercrimes. As observed in [15], a key goal of social work practice is to engage people and structures in the society with the aim of confronting and redressing life challenges and enhancing wellbeing. Social work practice features critical skills and capacities to identify essential changes in laws and policies to meet the needs of society members and communities, and to achieve justice. Social work is particularly important and impactful owing to its special role and focus on shaping the socioeconomic and political landscape of a society to promote the quality of life, wellbeing, and development of all society members, in line with the principles of social justice, inclusion, and equity [15] [4]. This role and focus of social work is relevant to the field of cyber-security to ensure the development and implementation of laws, policies, and programs to empower and protect all community members, including vulnerable people and communities such as children and youths, effectively from cybercrimes.

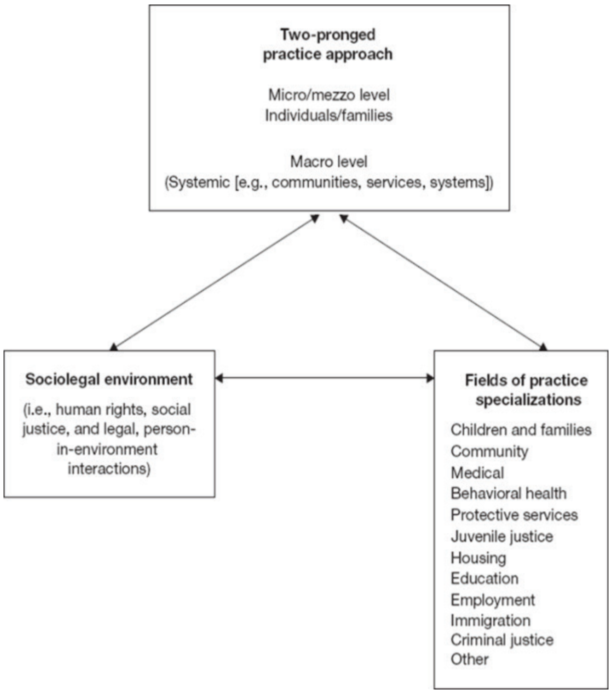

Fig. 3. A representation of the two-pronged approach to social work

Social work's focus on understanding, evaluating, and redressing the needs, experiences, and environments of individuals and communities through policies and laws aimed at social justice is particularly essential to help address cybercrimes targeting vulnerable communities and individuals, such as youths and children. Integrating social work practice in cyber-security programs and initiatives could help to orient these programs and initiatives toward the efforts and goals of addressing and alleviating the disproportionate impact of cybercrimes on vulnerable groups and people, such as children and youths, in the society. In particular, it would help to enhance these programs' responsiveness to the critical experiences of these vulnerable groups through tailored interventions and plans aimed at protecting and empowering them effectively against these crimes.

The forensic aspect of social work presents further critical value in the productivity of this field in cyber-security programs. As established in [18] and [19], social workers' roles today involve navigating the legal system and collaborating with diverse stakeholders within this system to create effective and lasting social change with positive and practical impact on communities and individuals. Fig.3 above shows a two-pronged approach to social work practice that requires these professionals to engage effectively in the legal environment [19]. This role helps these professionals to exert influence on legal systems, through education, advocacy, and proactive contributions to the development and implementation of impactful policies, and empower society members to solve their problems and improve their lives [19]. Forensic social work is essential to create practical interventions at the individual/micro, mezzo (group/household), and macro/systemic (organizational, institutional, cultural, societal, and community) levels, in line with the goals of enhancing people's individual functioning, coping, and problem-solving capabilities, linking clients to necessary resources, improving social service-delivery networks, and promoting social justice through social policy development and implementation [19]. These roles of forensic social work involve decision-making and actions based on critical risk assessments and evaluations of the vulnerabilities of specific populations. Additionally, social work could help to understand and evaluate the motives, goals, and behaviors of cybercriminals. Based on this insight, these professionals could help cyber-security programs to deduce and develop tailored strategies, plans, and protection and defense systems for specific social groups.

Alongside the forensic aspect, clinical social work enhances the success of cyber-security programs by availing critical insight into the behaviors, mindsets, and experiences of vulnerable communities. Clinical social work focuses on diagnosing, assessing, treating, and preventing mental, emotional, and behavioral disturbances among clients [19]. This aspect of social work could help to integrate considerations of the unique needs and experiences of vulnerable groups in cyber-security programs, thus enhancing the protective and defensive value and impact of these programs for these vulnerable groups. The value of clinical social work is especially relevant to this goal in cyber-security in terms of creating practical programs of empowerment and protection to alleviate the exposure of these groups to cybercrimes.

E. Social Work Practice and Community Development

Social work's critical role in cyber-security relates to its value and impact in community development. As established in [20], community development involves social change interventions aimed at the empowerment of community members to take collective action on issues of their interest, solve their problems, and improve their lives. Community development aligns with the nature of social work as a practice-based discipline whose goal is to promote social justice, respect for and achievement of human rights, and the empowerment of individuals and local communities [20]. While social change is a key goal of social work, community development incorporates further goals relating to the enhancement of participative democracy, economic opportunity, and sustainable development. In essence, community development involves the obligations of social workers to work in close partnerships with local communities and organizations to promote social and political action, policy development, and the achievement of human rights and social justice [20]. These focuses of social work in community development are essential to facilitate the empowerment of individuals, households, and entire communities, and to address problems of exclusion and violations of human rights and social justice.

Community development represents another important foundation of the value of social work practice in cyber-security. As established in [20] and [21], community social work focuses on the building of an inclusive environment for the integration and empowerment of community members in a society and its overall wellbeing and prosperity. The roles of social work professionals in this focus of community development include risk assessments, and policy analyses, development, and changes/improvements [21]. These roles involve efforts to investigate, analyze, and evaluate the root causes of social issues, and the unique environments and experiences of community members with regard to these issues. As noted in [21], some of the important roles of social workers in community development are the provision of counseling to individuals and families/households, development and conduction of support groups, community need assessments, community wellbeing planning, and the planning, development, and evaluations of community programs. Others include policy program analysis, provision of specialized cultural, service, and program activities to meet community needs, advocacy to raise and employ relevant resources to meet community needs, working with volunteers to support and enhance community programs, and advocacy to enact change at the structural level, including through contributions to relevant policies and law changes and improvements [21]. These roles of social workers are vital to inform advocacy, education, policy development, and other empowerment programs/interventions to serve local communities and address their needs and problems. These roles, processes, and goals of social work in community development are important pathways to enhance cyber-security policies and interventions at the level of local communities. In effect, community development represents an important way of empowering local communities to protect themselves from cybercrimes through education, advocacy, policy development, and the proactive involvement of their members and households in positive social change and relevant sociopolitical, cultural, and other actions aimed at defending and protecting them from these crimes. In these ways, social work's activities and responsibilities in community development represent a valuable means for the empowerment of local communities in cyber-security programs.

F. Significance of the Review

The review above supports the special value and role of social work as a field in enhancing cyber-security programs in today's world. It shows that specific social work practices and fields – the person-in-environment and HBSE approaches, community development aimed at positive social change, social work policy practice, forensic social work, clinical social work, and community development –support proactive, sustainable, and highly impactful cyber-security programs. Each of these areas/fields of practice in social work provides significant extra value through holistic assessments of the needs, experiences, environments, and processes of cyber use among individuals, communities, and society to inform strong cyber-security interventions. These practices are valuable for their emphasis on empowerment, policy improvement and development, and practical applications with just benefits for all users. The person-in-environment and HBSE frameworks of social work enable competent assessments of the experiences, needs, and environments of cyber-space from the perspectives of users, while community development practice in this field offers relevant and highly impactful paths of users' empowerment in cyber-security programs. Social work policy practice offers these programs the advantages of developing and improving policies and laws aimed at protecting and empowering individuals and vulnerable communities, such as children, from cybercrimes. On their part, forensic and clinical social work offer the programs key resources to navigate through and exert influence on legal systems through education, advocacy, and proactive social contributions to the development and implementation of impactful policies to empower communities and vulnerable groups with capacities to confront and solve their cyber-use problems and improve their cyber lives. Together, these aspects of social work promise to enhance the capacities of cyber-security programs to address the cyber-security needs of individuals and communities proactively, effectively, and sustainably (by providing an effective, long-term solution). In essence, the review demonstrates and proves the special value of social work and its approaches and fields in providing a critical path to harness and integrate the human element of cyber-space in cyber-security programs, thus fortifying these programs and ensuring their practical value in securing users and communities from cybercrimes and threats.

V. Discussion

Two key findings are evident from the review of evidence in published sources above. The first finding is confirmation of the special value of social work in fortifying cyber-security programs in today's world. The review confirms that social work's focus on situating, understanding, and evaluating the needs and experiences of individuals and communities in terms of their interactions with their environments presents special extra value in enhancing the practical quality, value, and impact of cyber-security programs and interventions. As evident in [3], [11], [12], and [22], effective cyber-security today requires proactive approaches to the needs and experiences of cyber-users based on a competent understanding of the psychological, sociological, and environmental influences behind their choices and behaviors in the cyber-space. It requires a competent understanding of the ways in which individuals and communities utilize, navigate through, and interact with the cyber-mediated information space in their daily lives. Critical considerations of current and evolving human factors and processes, including the complex processes of interactions between technology and human belief-thought-behavior patterns, are vital in proactive, impactful, and sustainable cyber protection, detection, response, and recovery programs [7]. The review illustrates that social work offers a key pathway to achieve this goal in cyber-security through its unique capacity to mobilize and provide competent and useful knowledge about the psychological and environmental factors and processes of human behavior that underlie cyber-security.

The second key finding is that specific foundations, practices, and fields or areas of social work have unique value in proactive and impactful cyber-security programs for users and communities in today's society. These foundations and fields/areas are the person-in-environment and HBSE frameworks, social work policy practice, forensic social work, clinical social work, and community development. As evident in [2], [4], [5], and [14], the person-in-environment and HBSE models orient social work toward holistic assessments of individuals' and communities' needs, environments, and behaviors based on recognition of the contributing roles of complex factors in their lives and social environments in their decisions, behaviors, and well-being. Social work policy practice focuses on developing and enforcing policies, interventions, and programs aimed at positive social change and the empowering and protecting vulnerable individuals and communities [4] [15]. Forensic social work involves social work professionals' duty to engage legal systems and exert influence on them to promote policies and actions aimed at empowering individuals/communities to meet their needs and problems [18] [19]. On its part, community development focuses on social change interventions to promote collective and impactful actions and the empowerment of communities to solve their problems [20] [23]. As Fig.4 below illustrates, these aspects and processes of social work are valuable in cyber-security as they base its programs and interventions on critical and holistic assessments of the needs and experiences of individuals/communities, thus informing competent policies, software development and applications, and impactful protection, defense, empowerment, and community development programs in the cyber-security effort. Collaborations between social work and information/computing sciences based on these foundations and fields of social work provide an important pathway toward more effective, productive, sustainable, impactful, and socially just cyber-security programs in modern society.

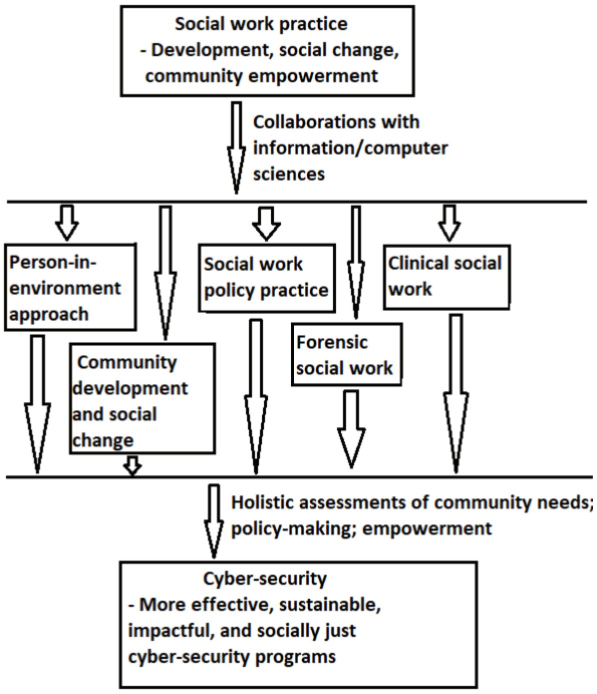
Social work practice
- Development, social change, community empowerment
Collaborations with information/computer sciences
Person-in-environment approach
Social work policy practice
Clinical social work
Community development and social change
Forensic social work
Holistic assessments of community needs; policy-making; empowerment
Cyber-security
- More effective, sustainable, impactful, and socially just cyber-security programs

Fig. 4. Value/impact of various foundations/fields of social work in enhanced cyber-security programs

One implication of findings in this review relates to the applicability of social work-informed cyber-security programs and interventions in diverse institutional and social settings to meet the needs of particular groups and populations. Social work, by its nature, is highly flexible, depending on the unique needs, experiences, and environments of people and communities. As established in [23], [24] and [25], social workers are productive and impactful in diverse fields and environments, which supports the adaptability of this profession and its capacity to provide tailored solutions for the unique needs of diverse populations and groups in the society. The key to success for social workers in these diverse settings lies in their competent interactions and partnerships with the populations that they serve to understand their needs and tailor solutions to these needs [24]. In this context, the value and impact of social work in cyber-security is unlimited, applying even in non-traditional settings such as schools and the international space. The foundations and fields of social work, as discussed above, could present optimum value in the productivity and impact of cyber-security programs in these settings through competent collaborations with relevant stakeholders, including target communities and local organizations. In the school setting, for instance, social work could provide unique insights into the unique needs and psychological and environmental experiences of students and school staff in their interactions with technology and in the cyber-space, as well as their vulnerabilities as a group or population in this space. This insight could inform tailored cyber-security interventions and programs in the school setting, which the social security field could also help to implement through its person-in-environment and HBSE models, community development resources, forensic and clinical aspects, and policy-making and positive social change and development roles.

Another key implication of the findings in this review concerns the applicability of social work as a foundation for cyber-security systems and interventions for diverse needs and populations. Social work insight into human, psychological, environmental, and sociological factors in human-technology interactions in cyberspace could contribute to more productive and efficient software building and applications, policy-making, protection systems, community development programs, and the empowerment of individuals and organizations against cyber-threats and cyber-crimes for diverse needs and populations. This insight could inform cyber-security systems aimed at detecting and tracking cyber-criminals, anticipating and evaluating the motivations and goals of these cyber-criminals, evaluating the experiences of potential cyber victims (including vulnerable groups such as children and youths), and creating or developing efficient chatbot systems to advise and support diverse groups in their uses of the cyberspace. These possibilities indicate the fundamental and extensive value of social work in holistic, productive, and sustainable cyber-security interventions and programs for diverse needs, settings, and populations in the modern society. This value of social work is especially significant in the modern age of complex and highly evolving needs, motivations, and experiences among both cyber-criminals and cyber-users in the society. Integrating social work in cyber-security programs is essential to hone the impact and responsiveness of these programs to the diverse and complex needs and experiences of cyber-users in today's society.

VI. Conclusion

Rather than being a purely technical domain, cyber-security is a complex and multi-dimensional issue requiring a comprehensive understanding and evaluation of human behavior, social dynamics, and prevailing organizational structures. These evaluations are necessary given the increasingly sophisticated nature of cybercrimes in today's society. Cybercrimes and their processes, goals, and effects occur in the context of environmental, psychological, and sociocultural factors and experiences among individual users and in human communities.

Two key findings are evident in this study. The first one is proof of the special extra value of social work as a field in enhancing the efficiency, impact, and sustainability of cyber-security programs in today's world. This value rests on this field's unique capacity to mobilize and integrate useful insight into the human element of cyberspace in cyber-security programs and interventions. In the face of highly evolving cyber-crimes and threats in today's society, the human component, in terms of human behaviors, choices, and interactions with and in the cyber-space, represents a front-line area of focus in effective cyber-security interventions. Social work provides a key pathway to harness and integrate the human element of cyber-space in cyber-security programs; it represents opportunities to make cyber-security programs more proactive, impactful, and sustainable by modeling these programs on the practical needs and experiences of users and communities. The second finding is that particular social work approaches have specialized value in competent cyber-security programs. These approaches are the person-in-environment and HBSE frameworks, social work policy practice, forensic and clinical social work, and community development. These approaches support holistic and evidence-based assessments of the needs, experiences, and environments of individuals and communities in the cyber space to enable impactful interventions aimed at their empowerment with capacities and resources to confront and solve their problems and needs in the cyber-space. These approaches are valuable for integrating the needs and experiences of diverse social groups, including vulnerable groups such as children, to enable advocacy, education, and policy-making interventions designed to meet their unique needs.

Effective collaborations between social work and information/computing sciences are necessary to harness this discipline's value in cyber-security. These collaborations could help develop social work-informed cyber-security programs and interventions in diverse institutional and social settings to meet the needs of particular groups and populations. They could contribute to more productive and efficient cyber-security mechanisms – including software building and applications, policy-making, protection systems, community development programs, and the empowerment of individuals and organizations – that align with the daily needs and experiences of individuals and communities in the cyber-space. These collaborations are an important foundation of genuinely effective, responsive, impactful, empowering, and sustainable cyber-security interventions in the face of evolving cyber-threats/crimes in today's society.

Conflict of Interest

Authors declare that they have no conflict of interest.

Funding

This article did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

References

[1] Arceneaux, and M. Harman, "Social cyber-security: A policy framework for addressing computational propaganda", *Journal of Information Warfare*, vol.20, no.3, 2021. https://www.jinfowar.com/journal/volume-20-issue-3/social-cybersecurity-policy-framework-addressing-computational-propaganda

[2] J. Burton, and C. Lain, "Desecuritisingcybersecurity: Towards a societal approach, *Journal of Cyber Policy*, 2020, doi: 10.1080/23738871.2020.1856903

[3] S. R. Muller, and D. N. Burrell, "Social Cyber-security and Human Behavior", *International Journal of Hyperconnectivity and the Internet of Things*, vol. 6, no. 1, pp. 1-13, 2022, doi: 10.4018/IJHIoT.305228.

[4] J. W. Bullee, and M. Junger, Social engineering, in T. Holt, and A. M. Bossler, Ed., The Palgrave handbook of international cybercrime and cyber-deviance, Geneva, Switzerland: Springer Nature Switzerland, 2019, doi: https://doi.org/10.1007/978-3-319-90307-1_38-1

[5] N. Duarte, N. Coelho, and T. Guarda, *Social engineering: The art of attacks*, 2021. https://comum.rcaap.pt/bitstream/10400.26/38593/1/paper17.pdf

[6] Z. Wang, L Sun, and H. Zhu, "Defining social engineering in cyber-security", *IEEE Access*, vol. 8, pp.85094-85115, 2020, doi: 10.1109/ACCESS.2020.2992807

[7] H. Loiseau, D. Ventre, and H. Aden, *Cybersecurity in Humanities and Social Sciences: A Research Methods Approach*. Hoboken, NJ, USA: Wiley, 2020.

[8] V. Koutroubas, and M. Galanakis, "Bandura's social learning theory and its importance in the organizational psychology context", Psychology Research, vol.12, no.6, pp.315-322, 2022, doi: 10.17265/2159-5542/2022.06.001

[9] T. Mogashoa, "Applicability of constructivist theory in qualitative educational research", *American International Journal of Contemporary Research*, vol. 4, no. 7, pp. 51-59, 2014.

[10] V. I. Akpan, U. A. Igwe, I. B. Mpamah, and C. O. Okoro, "Social constructivism: Implications on teaching and learning", British Journal of Education, vol. 8, no. 8, pp.49-56, 2020, https://www.eajournals.org/wp-content/uploads/Social-Constructivism.pdf

[11] K. M. Carley "Social cyber-security: An emerging

science", *Computational and Mathematical Organization Theory*, vol.26, pp. 365-381, 2020, doi: https://doi.org/10.1007/s10588-020-09322-9

[12] K. Carley, *The science of social cyber-security*. MobiCom 18, New Delhi, India, 2018. https://dl.acm.org/doi/pdf/10.1145/3241539.3241587

[13] M. F. Diaz, A. Charry, S. Sellitti, M. Ruzzante, K. Enciso, and S. Burkat, "Psychological factors influencing pro-environmental behavior in developing countries: Evidence from Colombian and Nicaraguan students, Frontiers in Psychology, vol. 11, 2020, doi: https://doi.org/10.3389/fpsyg.2020.580730

[14] N. P. Sharma, and V. Gupta, *Human behavior in a social environment*, Treasure Island, FL: StatPearls Publishing, 2024. https://www.ncbi.nlm.nih.gov/books/NBK574501/#:~:text=Psychological%20contributors%3A%20These%20include%20temperament,%2C%20socioeconomic%20status%2C%20and%20relationships.

[15] S. L. Burton, and P. D. Moore, "Pig butchering in cyber-security: A modern social engineering threat", *Socio-Economic Challenges*, vol.8, no.3, pp.46-60, 2024, doi: https://doi.org/10.61093/sec.8(3).46-60.2024

[16] International Federation of Social Workers, *Global definition of social work,* IFSW, n.d. https://www.ifsw.org/what-is-social-work/global-definition-of-social-work/ (accessed October 21, 2024)

[17] A. M. Syed, *Social engineering: Concepts, techniques, and security countermeasures*, 2021, doi: 10.48550/arXiv.2107.14082

[18] G. M. Tefera, M. Lembani, I. David, and W. Majee, "COVID-19 and migrant coping strategies: A person in environment perspective on experiences of Malawian migrants living in South Africa", *Journal of Social Service Research*, vol.49, no.4, pp.447-460, 2023, doi: https://doi.org/10.1080/01488376.2023.2236140

[19] C. Munson, "Forensic social work practice standards: Definition and specification", *Journal of Forensic Social Work*, vol.1, pp.37-60, 2011, doi: 10.1080/1936928X.2011.541200

[20] T. Maschi, and G. S. Leibowitz, *Forensic social work: Psychosocial and legal issues across diverse populations and settings, 2nd edition*. New York, NY, USA: Springer Publishing, 2017.

[21] F. O'Brien, I. Hawthorne-Steele, K. M. Pascoe, R. Moreland, E. Cownie, and C. Killick, "Bridging the gap between social work and community development: Implementing a post-graduate training partnership", *Social Work Education*, 1–18, 2022, doi: https://doi.org/10.1080/02615479.2023.2252844

[22] Canadian Association of Social Workers, *Social work practice in community development*, CASW, n.d. https://www.casw-acts.ca/en/social-work-practice-community-development#:~:text=Role%20and%20responsibilities&text=Provide%20counselling%20to%20individuals%2C%20couples,develop%20and%20evaluate%20community%20programs (accessed October 21, 2024)

[23] Columbia University, New York, *The diversity of social work: How shared experiences shape the field*, Columbia University, 2023. https://socialwork.columbia.edu/news/diversity-social-work-how-shared-experiences-shape-field (accessed October 21, 2024)

[24] Spring Arbor University, *The importance of diversity in social work,* Spring Arbor University, 2024. https://online.arbor.edu/news/importance-diversity-social-work (accessed October 21, 2024)

[25] A. M. Syed, *Social engineering: Concepts, techniques, and security countermeasures*, 2021, doi: 10.48550/arXiv.2107.14082