The Future of Cybersecurity Workforce Development

Author: Khaled Abdelaziz bin Mohammed Almoughem
Student Ph.D. Cybersecurity in the USA
Email: St20152015st@gmail.com

Abstract

This paper will discuss the future of cybersecurity workforce development. Cybersecurity is a field that is increasingly becoming important in today's workplaces. Considering the rapid growth of technology, it is expected that the field of cybersecurity will change significantly in the future. As such, preparedness is needed to ensure that the future cybersecurity workforce is not hindered by a lack of training, resources, or technical expertise. The personality traits of a cybersecurity professional should be evaluated before the assumption of a given occupation to ensure that this professional is the best fit and possesses all skills, values, and values required for that post. Teamwork should be integral in future workforce development because, according to the current trend in different industries, being a team player is essential. Lastly, cybersecurity professionals should be trained to observe ethics and civic duty by being loyal to their employers. They should also prioritize continued learning because the cyber domain is ever-changing and requires flexibility and adjustment. This paper will first explore the cyber environment and highlight some of the challenges currently facing the area. Next, the most fundamental skills needed for the furtherance of this field will be covered. One area that will be the paper's focus will be the importance of social skills. The article will finally provide an overview of some of the anticipated changes that will take place in the area of cybersecurity workforce development.

Keywords: Cybersecurity, Workforce, Future, Social, Skills.

1. Introduction

According to the current trends in the digital world, people who work in the cyber domain require diverse skills and knowledge to handle all situations professionally and successfully. With the recent technological advancements in different sectors and fields, cybersecurity workforce development is expected to be altered. In this case, other aspects will be integrated to fill various gaps in the current cybersecurity workforce. All the workforce development in this field will also require the inclusion of contemporary elements. The cyber domain is complex, which presents a unique challenge in developing a holistic and skilled workforce. Cybersecurity is a current field because it has not existed for an extended period, and this implies that there needs to be more information has been developed regarding the different aspects it entails. In this case, people emphasize essential technical skills and ignore organizational and social skills, which are critical for success in all settings (Dawson, 2018). In the future, it is expected that the development of the workforce in this field will put more emphasis on social and organizational skills because they dictate the outcomes of different occurrences in different settings. The future development of the cybersecurity workforce will include more positions to ensure that all critical aspects are well covered and addressed.

This workforce will be developed so that all members are systemic thinkers and have strong communication abilities. They will also have an intense yearning to learn more and be team players. They will be expected to have a strong sense of civic duty and should have balanced social and technical skills. These skills are essential because the cyber domain is a vast multi-disciplinary field comprised of different disciplines, such as engineering, computer science, economics, law, and psychology. Therefore, the workforce in this field must possess diverse skills that entail more than dealing with online devices. The cyber domain is critical because, in the modern world, it impacts different facets critical for human beings ranging from electricity to transportation networks used by people every day. In this case, the cybersecurity workforce plays a huge role in supporting and defending these networks. It is critical to ensure that they receive the best development so that they can be able to deal with cyberattacks effectively (Dill, 2018). There is a need for more cybersecurity workers regarding the number of posts available for these workers.

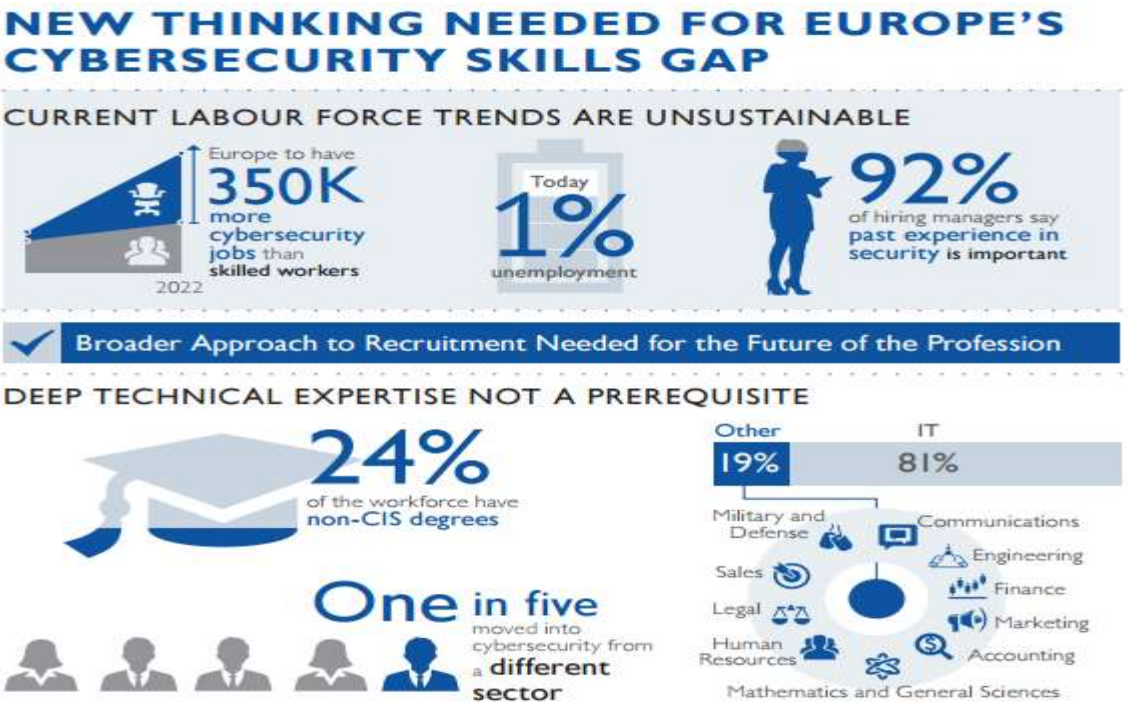

Figure 1: Gap in the cybersecurity workforce in the market

There is also a gap in the cyber domain and the skills necessary for a future workforce in this field. It is critical to examine this gap and evaluate different ways to address it to ensure that the cybersecurity workforce possesses all skills and knowledge essential in the future cyber domain.

2. Literature Review

Understanding the specific roles and responsibilities in any field is one of the most critical factors that can help shape the organization of a company's workforce. It is a fact that different people, especially cyber professionals, are different. However, it is the responsibility of every organization to ensure that all these individuals fit in an organization. Organizations should thus embrace systems aimed at developing their cybersecurity workforce and ensure that continuous learning processes are maintained in the long run. Technical expertise will undoubtedly be integral to a better cybersecurity landscape (Wang, 2019). It is a fact that this field is in its infancy, and much academic work remains undone. However, it is expanding rapidly, requiring advanced research critical to understanding these aspects. In this case, it is critical to understand what makes a proficient cyber professional and how to recruit such a worker.

It should also be noted that the fact that cybersecurity is an integral part of national security means that the defense forces are expected to be directly involved in the development of the systems and personnel that form the cybersecurity network.

Cyber Domain

According to Dawson (2018), the cyber domain is divided into three layers: social, physical, and logical. The physical layer includes the infrastructure and hardware that support different networks. The logical layer comprises different logical devices that are linked to a network. Examples of hardware that support the logical layer include Digital Cross-Connect Systems, Central Office switches, and Main Distribution Frames. The social layer comprises all cognitive aspects of different personas interacting within a network. Currently and in the past, people have been concentrating on logical and physical layers and ignoring the social layer because it is not connected to cybersecurity directly. In the future, the social layer will be given a higher consideration because people have different human interactions in different layers that make the cyber domain unique (Blair, 2019). Understanding these diverse human interactions is critical because they are the source of vulnerabilities on different networks. Therefore, the future of cybersecurity development, in-depth knowledge, and skills in human interactions will be emphasized. Also, advanced training in developing technologies such as Artificial Intelligence and quantum computing should be incorporated to ensure that the future workforce can handle such systems easily and manage them effectively.

NICCS Structure

The National Initiative for Cybersecurity Careers and Studies (NICCS) has a cybersecurity framework that provides information about the work roles of different people in the cybersecurity workforce. There are over 31 specialty areas and about 1000 types of skills and abilities (National Initiative for Cybersecurity Careers and Studies, 2020). However, these acting roles are based on traditional information technology. They maintain and operate roles, including security analysts, system administrators, and knowledge management. The govern and oversee roles include cyber law, education, policy development, and managerial roles. The defend and protect roles include network defenders and cyber analysts. The major challenge with NICCS role training programs is that less than ten skills include social skills and teamwork training. Therefore, as much as the advancement of technical skills training is essential, it is critical to incorporate different aspects related to the social fit of cybersecurity training.

One of the most critical aspects that NICCS should consider in the future is to develop talent based on the different traits of trainees (Thomson, 2018). According to past cyberattacks, it was discovered that human behavior was exploited, and therefore social factors should be incorporated into future cybersecurity workforce development. The framework provided by NICCS includes a wide array of skills, knowledge, and abilities that form the training program's crust. The organization collaborates with various learning institutions to ensure these skills are passed to as many trainees as possible. However, many colleges need to align with the set curricula, and these limitations threaten the qualities needed in a cybersecurity workforce.

Challenges Facing the Current Development Framework

The main problem with the current training programs is that they emphasize electrical engineering and technical skills. Social skills should be prioritized because the skills and knowledge developed are essential in developing effective teams. They are also crucial because they ensure greater fidelity in developing a holistic cybersecurity workforce. In this case, it is essential to define the right organizational environment to ensure that an effective cybersecurity workforce is produced. The current structure of different institutions that offer different programs needs to be completed because they need to offer comprehensive training in work roles and attributes (Mailloux, 2018). A changing work environment characterizes the cyber domain, and the needed skills are also changing. In this case, introducing motivational and social metrics is essential to ensure that cyber professionals can overcome various challenges related to several social factors.

3. Analysis

Different studies have concluded that more than technical knowledge for cyber professionals is required because a lack of social skills leaves a security, retention, and knowledge gap. Therefore, a significant gap exists in the current NICCS framework, which needs to be completed because there is a need for a cyber-professional with communication skills efficient in making savvy decisions and managing other members in an organization. With the current technological advancement and development of the number of cyberattacks, cybersecurity should be prioritized so that different members of an organization are trained or have essential information in this field. Studies and research papers that have been done in the past have yet to cover cybersecurity professionals' organizational and social fit. It is also critical to ensure that cybersecurity professionals receive continuous education because supplemental education ensures they remain proficient. In the future, there should be different programs designed so that cybersecurity professionals receive supplemental education after a particular period. The future of cybersecurity workforce development should prioritize on-the-job training and mentorship because the cyber domain keeps experiencing different changes (Sharevski et al., 2018). This requires cybersecurity professionals to keep updating their knowledge and skills in dealing with new technologies.

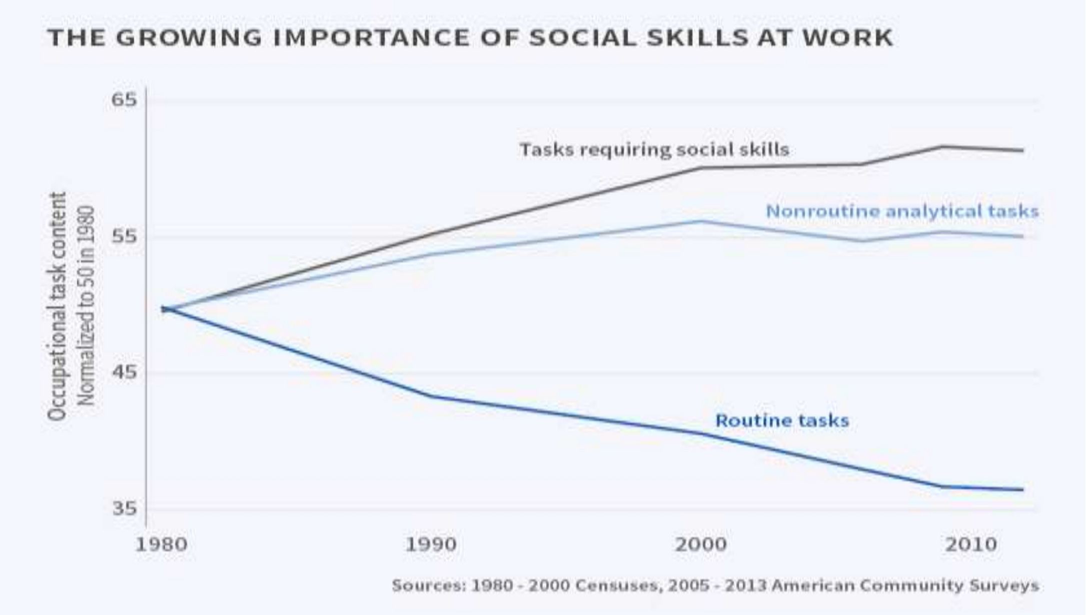

Figure 2: Need for social skills in cybersecurity

Importance of Social Skills

The nature of cybersecurity work is complex, and professional cybersecurity needs to be trained to work in teams. This is important in different organizations because different teams require diverse talents. In the private sector, the cybersecurity department only comprises a small number of workers. A cybersecurity worker must have ample knowledge and skills to ensure that different areas are covered and safeguarded. Distribution of expertise is critical in cybersecurity, and corporations should be keen to observe this aspect in their cybersecurity teams. The current demands in the cyber domain require a holistic team of professionals with diverse knowledge in different areas. Therefore, future cybersecurity workforce development programs should prioritize developing high skills related to teamwork and collaboration (Dawson, 2018). The social aspect of the cyber domain is clinical, and the current systems have neglected this aspect.

In this case, the future program should account for social and technical skills to achieve excellence and true creativity. The complexity of the cyber domain is a significant problem that cybersecurity professionals face, and it is critical to address this problem in the future. People from other departments that do not deal with cybersecurity aspects have difficulty dealing with the language used in this field. This requires changing the entire educational system, where cybersecurity is introduced as a standard unit in different courses.

Cybersecurity Needs

Currently, organizations are characterized by tightening budgets, and they cannot hire a cybersecurity team and have to work with an individual. According to Swarovski et al. (2018), this is a serious issue because some organizations do not understand their cybersecurity needs. Therefore, as much as teamwork is emphasized, it is critical to ensure that individual cybersecurity professionals can handle essential aspects related to the overall requirements of a small organization. Another area that needs to be addressed in the future is developing an ethical code that will ensure that cybersecurity professionals follow different directives that ensure that an organization's networks and information are safeguarded from exploitation (Sharevski et al., 2018). Cybersecurity professionals should be trained to create and maintain high levels of trust with their organizations and employers. This is critical because cybersecurity professionals remain the highest threat to organizational data if their loyalty is divided. Therefore, future cybersecurity workforce development should prioritize the development of values and technical skills. The value system is critical and should be encoded in law to ensure that cybersecurity professionals have a high moral standing related to duty obligation and law adherence. The relationship between cybersecurity professionals and organizational management should be based on the assumption that these professionals will conduct their obligations in good faith.

Current Trends in the Cyber Domain

Top organizations around the globe ensure that their top management has ample technical knowledge and takes measures necessary to assess how managers are performing. There is no doubt that, in the future, it will be imperative to develop robust cybersecurity workforces that will be able to address the constantly emerging cyber issues. There will be many people whose cybersecurity skills will need to be substantially improved. The training capacity for various professions related to cybersecurity needs to be broadened.

It will be essential to encourage higher learning institutions to take this opportunity and explore ways to offer such courses to their students. Not all cybersecurity professionals fit in an organization, and it is critical to train these professionals to deal with diverse situations and work environments. In this case, the inclusion of social skills in training is essential because it enables cybersecurity professionals to fit in different work environments and to remain trustworthy and reliable (Crumpler, 2019). Cybersecurity professionals seek to work for organizations that fit their values, skills, and knowledge because they have yet to be trained or equipped with social skills. As much as cybersecurity professionals seek job satisfaction, they should be trained to deal with different aspects of the organizational culture of diverse organizations. For example, cybersecurity employed in a hospital should have diverse skills to deal with the complexities associated with such an organization.

4. Discussion

In the future, cybersecurity should be trained to deal with situational dynamics within different organizations. Cybersecurity professionals need help adjusting and blending into different organizations because they need to possess the required social skills. The Big Five Personality traits model is one of the tools used to determine a person's aspects. It can identify cybersecurity professionals who can thrive in different settings. Therefore, understanding the cyber domain is essential because it helps identify the occupational classifications that individuals fit in perfectly according to their personality traits. In the future, it is critical to have a program that helps cybersecurity professionals identify the area they fit best before specializing in different areas. This will ensure that cybersecurity professionals specialize in areas that fit their traits and where they can produce optimal results (Caulkins et al., 2016). The other aspect that should be addressed is the emerging roles in the cyber domain, which is experiencing continuous change. The future cybersecurity workforce development should be shaped by the predicted organizational work based on the technological advancement expected shortly. Cybersecurity professionals are facing a huge challenge related to a need for more content comprehension because there are aspects they need to understand because they were not present in their training. To address this issue, it is critical for the current and future training programs to entail the content of different cybersecurity issues that are expected to be experienced shortly.

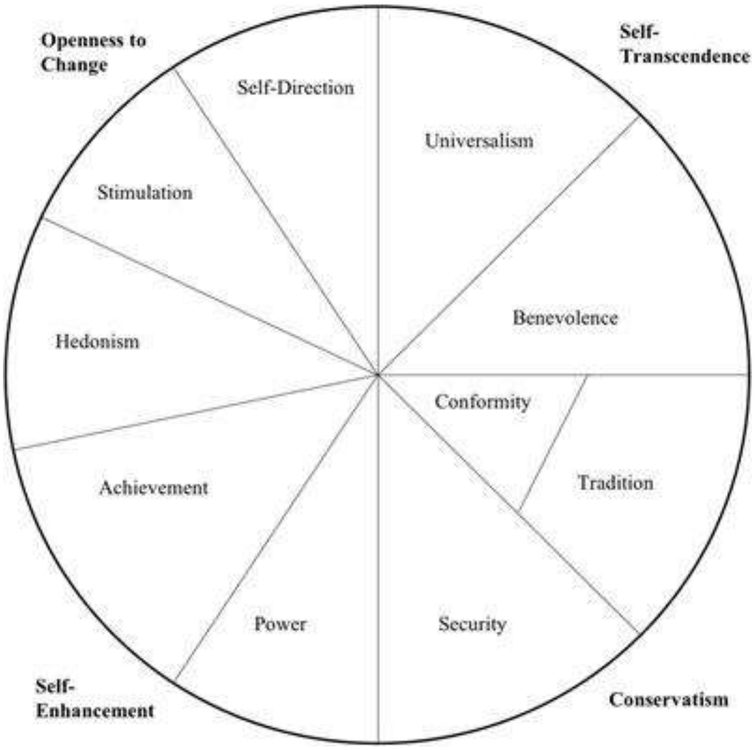

Figure 3: Social skills needed in cybersecurity

Incorporation of Social Skills and Teamwork

As stated, it is critical to understand the cyber domain, and future cybersecurity workforce development should encompass all relevant aspects of the current cyber domain. Also, cybersecurity professionals should be trained on how to strengthen their predictive power because cybersecurity requires vigilant people who can predict potential attacks and threats. These professionals should also have the skills necessary to offer valuable insights, which should also be related to the occupational interest of trainees. The future of the cyber domain requires systemic thinkers, and the development of these professionals should ensure that they can link the interconnections between different elements effectively (McDuffie, 2014). They should also be able to deal with the cyber domain as a system of structures by applying mental agility and the current conceptual framework. Being a team player is essential for a cybersecurity professional, and it requires him/her to have excellent skills required in a cyber-team. The future is founded on working in teams, and the objective will be to establish a team that produces high performance.

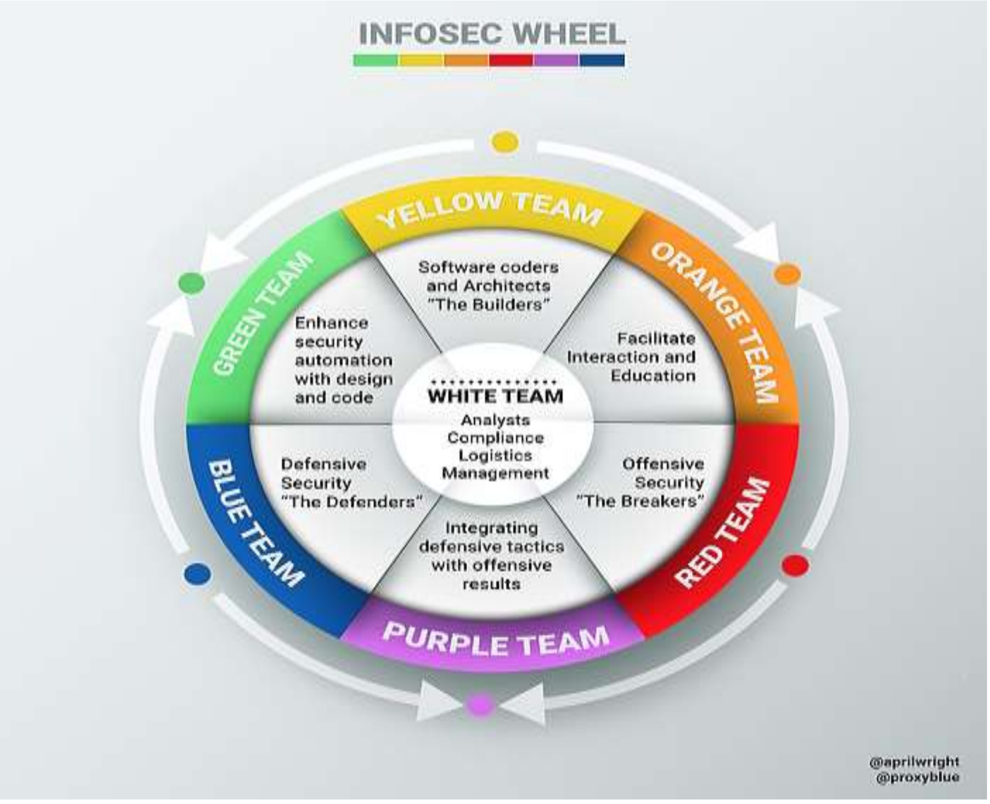
INFOSEC WHEEL
YELLOW TEAM
Software coders and Architects "The Builders"
ORANGE TEAM
Facilitate Interaction and Education
RED TEAM
Offensive Security "The Breakers"
PURPLE TEAM
Integrating defensive tactics with offensive results
BLUE TEAM
Defensive Security "The Defenders"
GREEN TEAM
Enhance security automation with design and code
WHITE TEAM
Analysts
Compliance
Logistics
Management
@aprilwright
@proxyblue

Figure 4: Teamwork in cybersecurity

5. Conclusion

The future of cybersecurity workforce development depends on different aspects that make the current development programs ineffective. One of the issues that have been found critical is the inclusion of social skills in the development of this workforce. Social skills are critical in the same way as technical skills are because cybersecurity professionals work in an environment where human aspects contribute to the outcomes of different tasks. Social skills training is needed to complete the current training programs offered by NICCS, and they should be incorporated in the future. Future security workforce development should encompass training in emerging technologies applied by different organizations, such as quantum computing and AI. The personality traits of a cybersecurity professional should be evaluated before the assumption of a given occupation to ensure that this professional is the best fit and possesses all skills, values, and values required for that post. Teamwork should be integral in future workforce development because, according to the current trend in different industries, being a team player is essential. Lastly, cybersecurity professionals should be trained to observe ethics and civic duty by being loyal to their employers. They should also prioritize continued learning because the cyber domain is ever-changing and requires flexibility and adjustment.

6. Glossary

Cyber domain: This is a global realm within the information landscape where interdependent networks of information and data are found.

The physical layer**:** The infrastructure and hardware that support different networks.

The logical layer**:** Comprises different logical devices that are linked to a network.

The social layer*:* Comprises all cognitive aspects of different personas interacting within a network.

NICCS**:** National Initiative For Cybersecurity Careers And Studies

7. Academic Integrity Statement

The independent pursuit of information and knowledge is an essential part of education. I also acknowledge that academic integrity is an integral part of the code of conduct of our university. Therefore, I have committed myself to upholding this code, and as such, all the work presented in this paper is my own, and I have given credit where due, with proper citations and referencing.

8. References

Blair, J. R., Hall, A. O., & Sobiesk, E. (2019). Educating future multi-disciplinary cybersecurity teams. *Computer*, *52*(3), 58-66.

Caulkins, B. D., Badillo-Urquiola, K., Bockelman, P., & Leis, R. (2016, October). Cyber workforce development using a behavioral cybersecurity paradigm. In *2016 International Conference on Cyber Conflict (CyCon US)* (pp. 1–6). IEEE.

Crumpler, W., & Lewis, J. A. (2019). *Cybersecurity Workforce Gap*. Center for Strategic and International Studies (CSIS).

Dawson, J., & Thomson, R. (2018). The future cybersecurity workforce: Going beyond technical skills for successful cyber performance. *Frontiers in Psychology*, *pp. 9*, 744. Retrieved from https://www.frontiersin.org/articles/10.3389/fpsyg.2018.00744/full

Dill, K. J. (2018). Cybersecurity for the nation: workforce development. *The Cyber Defense Review*, *3*(2), 55–64.

Mailloux, L. O., & Grimaila, M. (2018). Advancing cybersecurity: The growing need for a cyber-resiliency workforce. *IT Professional*, *20*(3), 23-30.

McDuffie, E. L., & Piotrowski, V. P. (2014). The future of cybersecurity education. *Computer*, (8), 67-69.

National Initiative for Cybersecurity Careers and Studies. (2020). About NICCS. Retrieved July 31, 2020, from https://niccs.us-cert.gov/

Nunius, J. (2017). Cyber security skills shortage to hit 1.8 million by 2022. https://www.cbronline.com/cybersecurity/protection/cyber-security-skills-shortage-hit-1-8-million-2022/

Piccard, P. (2019). Infosec Wheel. https://www.pinterest.com/pin/174373816808404679/

Picker, L. (2015). How important are social skills at work? https://www.weforum.org/agenda/2015/11/how-important-are-social-skills-at-work/

Sharevski, F., Trowbridge, A., & Westbrook, J. (2018, March). A novel approach for cybersecurity workforce development: A course in secure design. In *2018 IEEE integrated STEM education conference (ISEC)* (pp. 175–180). IEEE.

Thomson, R., & Dawson, J. (2018). The Future Cyber Workforce: Defining the Domain and the Skills, Knowledge, Attributes Necessary for Successful Cyber Performance. *Frontiers in Psychology*.

Wang, P., & D’Cruze, H. (2019). Cybersecurity certification: certified information systems security professional (CISSP). In *16th International Conference on Information Technology-New Generations (ITNG 2019)* (pp. 69-75). Springer, Cham.

Doi: doi.org/10.52132/Ajrsp.en.2023.45.3