Inclusive and Accessible Cybersecurity: Challenges and Future Directions

Bilal Naqvi, Lappeenranta-Lahti University of Technology
Joakim Kävrestad, Jönköping School of Engineering
A.K.M. Najmul Islam, Lappeenranta-Lahti University of Technology

The article aims to examine the state of the art concerning cognitive accessibility in the design and development of cybersecurity systems and services. The findings reveal that despite recommendations toward cognitive inclusion, consideration toward cognitive disabilities during the design and development of security functions is nonexistent.

Cybersecurity systems and services are often cognitively demanding, while a significant portion of the population is experiencing a cognitive disability. A consequent lack of cognitive availability can result in digital inequality. Herein, 10 semistructured interviews were conducted with the security practitioners to identify the state of the art (from an industry's perspective) concerning cognitive accessibility.

COGNITION AND CYBERSECURITY

Humans are endowed with a diverse set of abilities; however, sometimes there are limitations and disabilities either from birth or developed during life. According to the World Health Organization's report on health equity for persons with disabilities, 1.3 billion people (16% of the total world population) experience disabilities.[1] Among these disabilities are cognitive disabilities and limitations. The term *cognitive disability* refers to a broad range of conditions, including intellectual disabilities, autism disorders, mental illness, brain injury, stroke,

Digital Object Identifier 10.1109/MC.2024.3376827
Date of current version: 3 June 2024

Alzheimer's disease, and other dementias.[2] The available stats reflect a high percentage of the population experiencing cognitive disabilities in their respective countries: for instance, a recent report by the U.S. Center for Disease Control and Prevention identifies that 12.8% of the adults in the United States experience cognitive disabilities. It is also relevant to state from the report that the number of people (12.8%) experiencing cognitive disabilities is more than those experiencing any other form of disability.[3]

Cognitive abilities involve perception and people's ability to solve problems, plan, and reason.[4] Concentration and memory are also cognitive abilities.[5] Furthermore, people's cognitive abilities are dynamic, and an individual can be impacted on a temporary or permanent basis.[13,14] Conditions that can permanently impact a person's cognitive abilities include autism, dyslexia, stroke, brain injury, and dementia.[2] Factors that can temporarily impact a person's cognitive abilities include stress and fatigue,[13] and how a certain condition will impact a person's cognitive abilities is highly individual.[15] However, a person with a cognitive disability will experience limitations in one or more of the cognitive abilities. These abilities are important precursors for cybersecurity behavior, where users are expected to follow security plans and procedures, reason and make decisions about the legitimacy of emails, create and memorize passwords, and more.[17] Moreover, cybersecurity tasks are often cognitively demanding with cybersecurity fatigue as a possible consequence.[11] Minimizing cognitive workload is an important usability factor for cybersecurity functions and interfaces.[12]

Cybersecurity and cognitive functioning have been previously studied from an accessibility perspective. For instance, Kävrestad et al.[18] describe that cognitively demanding cybersecurity tasks are "usability hinders" for users with cognitive disabilities and neurotypical users alike. However, the hindrances are often more severe for users with cognitive disabilities. A task that is perceived as a nuance by a neurotypical user may be impossible for a user with a cognitive disability to complete.[18] At a more detailed level, the extant literature demonstrates that cognitive ability impacts a user's ability to detect phishing[9] and use cybersecurity functions, such as captchas.[10] Furthermore, users with cognitive disabilities do have difficulties while authenticating using the current range of authentication options available: for instance, remembering complex passwords without writing them down can prove to be a cumbersome task for users with cognitive disabilities. Similarly, the use of biometrics, such as fingerprints, can be difficult for a user who has had a stroke resulting in disability or paralysis of arms and hands.[19] A pertinent aspect to consider is either to leave cognitively challenged users reliant on their caregivers to perform cybersecurity functions or to develop solutions that consider cognitive factors in the design and development of cybersecurity functions. Consequently, cognitively accessible cybersecurity is an important security matter, since it allows all users to efficiently use cybersecurity functions, and an important equality matter, since it is a crucial usability and accessibility aspect.

With the importance of cognitive accessibility in cybersecurity, and the apparent lack thereof in practice, a pertinent question to consider is: How is cognitive accessibility considered during the design and development of cybersecurity functions by security practitioners? It is relevant to mention that the term *cybersecurity functions* is used as an all-encompassing term for functions, features, and policies the users are expected to follow. Consider that the cognition aspect in cybersecurity is not just a research challenge, but also an equality and inclusivity concern because it works toward equal access to digital technology. This is identified by inclusivity goals, such as sustainable development goal (SDG) 4, SDG 8, SDG 10, SDG 11, and SDG 17 that demand inclusive and equitable strategies for all, including people with disabilities.[8] Nonconsideration of the cognitive accessibility in the design and development of cybersecurity functions can impact peoples' access to, for instance, online education facilities, health-care services, Internet banking, etc., all of which require interacting and managing cybersecurity functions.

This article advocates for the need to consider cognitive accessibility in the design and development of security systems and services not just to ensure usability of security, but also from an inclusion perspective. The article reveals the state of the art from the industry concerning the consideration of the same by the practitioners. The challenges that exist in this regard are also listed in the article. Furthermore, the article also presents the future directions for practitioners and policymakers to develop further course of action toward ensuring usable yet accessible and inclusive cybersecurity.

MATERIALS AND METHODS

Having discussed the cognition and cybersecurity perspective, the focus of this research is on identifying the state of the art concerning cognitive accessibility during the design and development of security functions. To do so, semistructured interviews with (n = 10) practitioners from the industry in Finland and Sweden were conducted. The interview protocol was developed with the following objectives in consideration:

- to identify the state of the art in the industry concerning consideration of cognitive disabilities in the design and development of cybersecurity functions for both the end-users and the company's employees
- to identify the future directions and avenues for inclusion of the cognitive disabilities in cybersecurity functions developed in the future.

Study protocol

The interviews were carried out semistructured as described by Robson and McCartan.[6] Given the exploratory nature of the main research question (that is: How is cognitive accessibility considered during the design and development of cybersecurity functions by security practitioners?), an interview guide was created with few but open questions on how the participants' organizations addressed cognitive disabilities when developing cybersecurity functions for their customers and employees, respectively. A purposive sampling approach was adopted with the intent of including participants who are decision makers regarding cybersecurity.[7] The research included participants working at companies active in Sweden or Finland, and who influenced cybersecurity decisions that impacted at least 100 users. Ten participants were recruited by approaching suitable candidates from the researchers' networks. Table 1 provides an overview of the interview participants. The interviews lasted half an hour (on average). The interviews were recorded for analysis purposes. The interview recordings were later transcribed and correlated with the notes taken by the researchers for analysis. Two researchers participated in each interview and transcribed half of the interviews each. The transcriptions were then reviewed by the other researcher. Ethical concerns were followed during the participants' recruitment and the interviews. Upon agreeing to participate in the interviews, the participants were presented with an informed consent where the full purpose of the research was disclosed. They were informed that they could withdraw from the study at any time and that they would remain anonymous throughout the research. When they accepted the conditions of the informed consent, an interview was booked and carried out using Microsoft Teams.

Data analysis and method

The Gioia method was used to analyze the interview data. The Gioia method is

TABLE 1. Details of the interviewees.

	Role	Company	Size	Location
1	IT manager	IT security consulting company	30 employees, 100 customers	Sweden
2	Managing director	Digital product development and service provider	Several hundred	Finland
3	Director information security	Software and services	Several hundred thousand	Multinational
4	Chief security officer	Public administration	7,500 employees, 50,000–100,000 users	Multinational
5	Chief information security officer	Security consulting company	1.3 million users	Sweden
6	Information security specialist	IT company	~75,000	Sweden
7	CEO	Information security cluster	80-member cybersecurity companies	Finland
8	System administration	IT services	5,000	Sweden
9	Business owner and entrepreneur	Delivering online services	300+	Finland
10	Product security specialist	Health-care IT and device services	Several thousand	Multinational (Finland)

an inductive qualitative data analysis technique.[16] Its inductive aspect, which enables generating broad generalizations based on informants' comprehension of the organizational activities, was one of the factors that led to its selection. In line with the specifics of the Gioia method, a three-stage analysis method was followed. First, the interview transcripts were examined, and then the audio recordings of the interviews were listened to. The goal was to assign first-order codes to the interview data. Codes were assigned to statements that were made repeatedly, unexpected responses, characteristics that interviewees emphasized, or information that was comparable to what

TABLE 2. Key concepts and associated codes during stage 1 of the analysis.

Concepts	Example of codes	Example quotes
Focus on cognitive disabilities	Support offered, nonexistent consideration, limited and specific focus	"To some extent. As end-users we discussed this, not about the technical part, in that part we offer support instead." "Actually no. If I think the industry where I've spent my career, so manufacturing industry, technology industry, this hasn't been a topic at all."
Reasons for lack of consideration	Specific requirements, legislations, standards, lack of market potential	"I think one of the answers is that it's not required it doesn't come as a specific requirement." "Monetary aspects are important. These types of research and development implemented different types of, let's say logging methods. It of course requires work, which means it requires money."
Some important considerations	Usability, accessibility, burnouts	"I think, first of all, we should improve general usability and accessibility." "I mean it makes sense, right? If you have someone who's, you know, unable to read properly or, you know, see the actual field they're going to ask someone else to log in, which, you know, kind of breaks."
Future directions	Raising awareness, financing initiatives, legislations, and sanctions	"I think some examples making it you know, because if we don't relate, if we don't understand, and then even if we would sort of understand that the topic is there like the diversity but before you get ideas how to start solving it some examples but also awareness and speaking about it." "I think there needs to be like legislation that says that everyone should be included even in the security aspect."
Involvement of roles	Senior managers, UX, marketing	"We should use all parts in the company senior and junior developers, it is UX, it is marketing and it's the IT department who does some testing. We cooperate on all fronts to get as good a product as possible."
Cognitively challenged employees	Security first policy, case-specific consideration, special gear	"We always put security first. And as said that cannot be discussed but we are included in supporting based on need instead. But our customers are as important as our internal, so it is important to maintain high security." "Currently handle those basically case by case and let's say if some employee would need some let's say special gear or something like that. We've kind of course looked at those and kind of taken care of it. I would say that we are going at its case by case."
Impact on security hygiene	Impact, important, critical	"Yes, it does impact. Because we are all important, we are all different. We all learn differently, and we all remember things differently. So yes, some people. May feel that they are not getting the information and not feel but they are not getting the information." "Yes, I think so. I wholeheartedly agree. Like when you when you do, when you source applications from third parties you want to make sure they're easy to use. But usually, the perspective is easy to use for an older person who doesn't have you know that much computer knowledge or experience with using particular software. I think that this perspective is something that needs to be considered before, at least not when I've done it right. Like there's usability for people with less knowledge, but there's not usability for people with enough knowledge, but the inability to use the system to its fullest potential."

UX: user experience.

had been recorded in other studies and connected to a theory or model.

FINDINGS

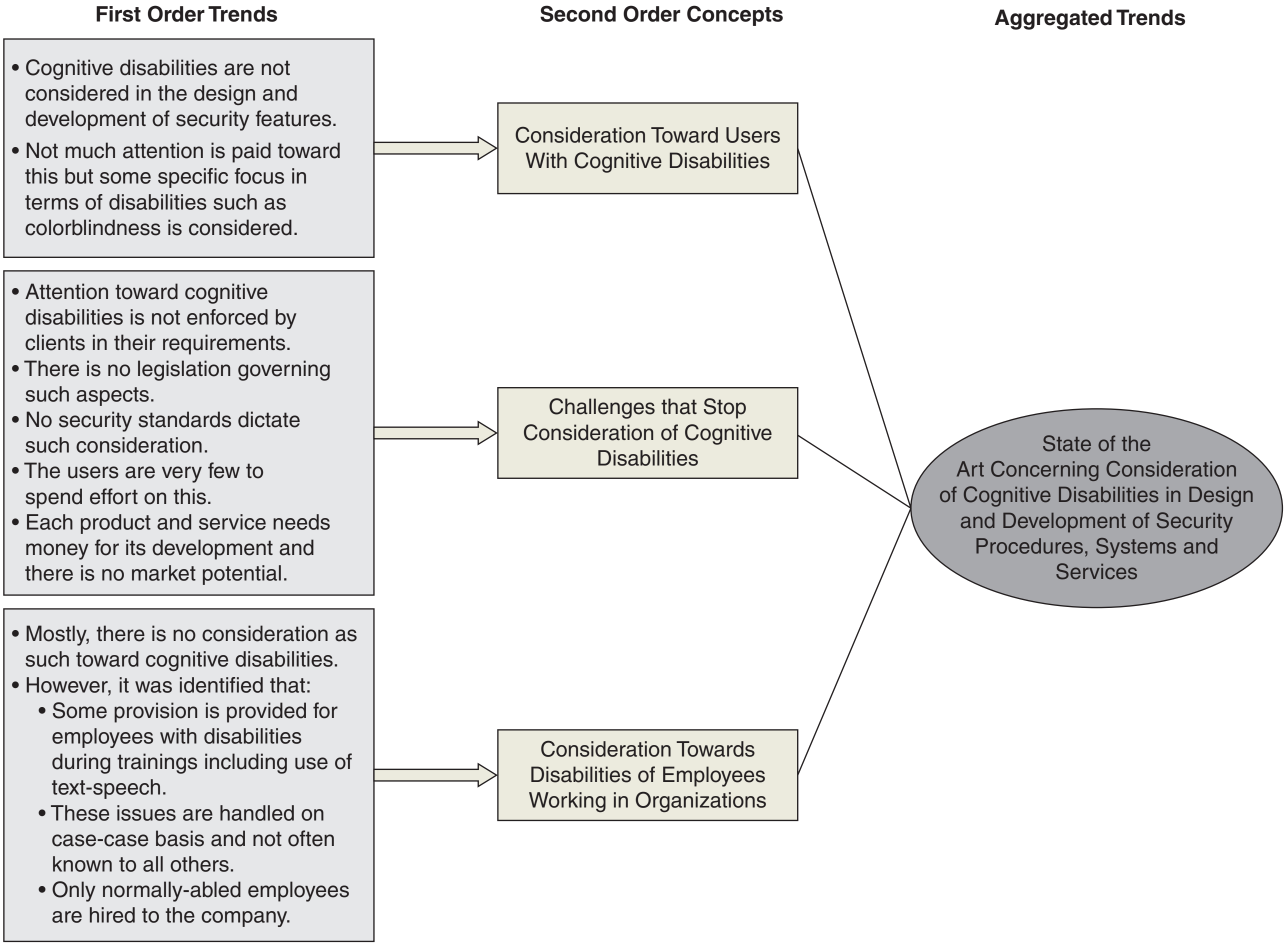
In line with the Gioia method, a three-stage method was followed. During stage 1, the codes that were created along with the example quotes by the interviewees are presented in Table 2.

After this exercise, the first-order trends were finalized. In the second stage, the related codes were merged to develop broader categories and abstract concepts. Finally, in the third stage, the second-order concepts were aggregated to form broader themes relevant to the research questions and objectives considered during these interviews. More details about the second and third stages of the analysis are presented in the subsequent sections.

State of the art unveiled

In line with the objectives framed for the interviews, three broad concepts are relevant to be discussed for representation of the state of the art. The second-order concepts and the aggregated themes from the perspective of the state of the art concerning consideration of cognitive disabilities in the design and development of cybersecurity functions are presented in Figure 1.

Consideration toward users with cognitive disabilities. It was revealed during the interviews with the practitioners that cognitive disabilities are not often considered during the design and development of cybersecurity functions. Although there are some considerations for disabilities, such as color blindness,



First Order Trends
Second Order Concepts
Aggregated Trends
• Cognitive disabilities are not considered in the design and development of security features.
• Not much attention is paid toward this but some specific focus in terms of disabilities such as colorblindness is considered.
• Attention toward cognitive disabilities is not enforced by clients in their requirements.
• There is no legislation governing such aspects.
• No security standards dictate such consideration.
• The users are very few to spend effort on this.
• Each product and service needs money for its development and there is no market potential.
• Mostly, there is no consideration as such toward cognitive disabilities.
• However, it was identified that:
• Some provision is provided for employees with disabilities during trainings including use of text-speech.
• These issues are handled on case-case basis and not often known to all others.
• Only normally-abled employees are hired to the company.
Consideration Toward Users With Cognitive Disabilities
Challenges that Stop Consideration of Cognitive Disabilities
Consideration Towards Disabilities of Employees Working in Organizations
State of the Art Concerning Consideration of Cognitive Disabilities in Design and Development of Security Procedures, Systems and Services

FIGURE 1. State of the art concerning consideration of cognitive disabilities.

the consideration toward cognitive limitations is nonexistent. When asked about possible reasons for this nonconsideration, several reasons (discussed below), such as lack of awareness and less market potential, were identified.

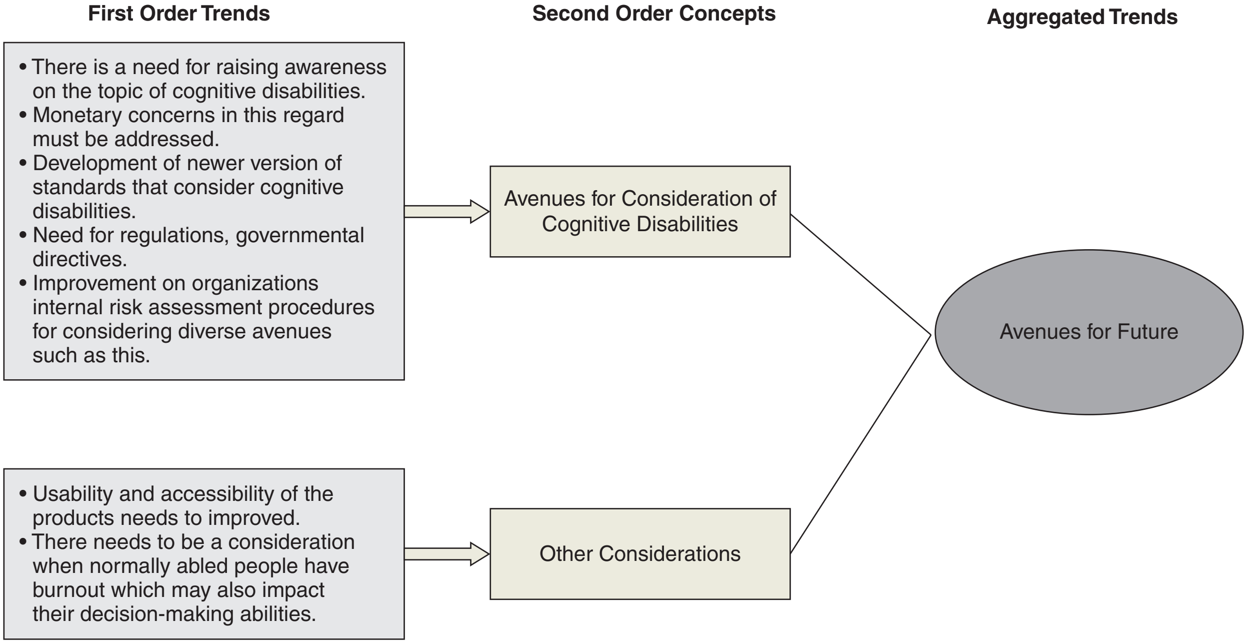
Challenges that limit consideration toward cognitive disabilities. When the state of the art revealed almost nonexistent consideration toward cognitive disabilities, the interviewees were asked about the possible reasons and challenges that limit such consideration. Among the challenges the interviewees reported, the following are the most important:

- The requirements for the products are driven by the clients, and cognitive accessibility requirements are not specified by the clients.
- Some legislations govern the use of software and security products and services in all regions of the world; however, there are no legislations as such that bind the development companies to develop products that consider such requirements.
- In addition to the legislation, the products need to comply with standards and regulations; however, there is a lack of recommendations by the standards that dictate consideration of cognitive disabilities.
- There is a lack of awareness on the topic and developing organizations are oblivious to the fact that their products will be used by users with cognitive disabilities; therefore, the products are developed without consideration of cognitive limitations.
- Finally, the industry is driven by funds and there is no market potential for investing such an effort and developing accessible products.

Consideration toward disabilities of employees. In line with one of the objectives of this study, the interviewees were asked specifically concerning consideration of cognitive disabilities that one of their employees faces. The goal was to identify any provision in the security policies and procedures for employees with cognitive disabilities. It was revealed that there are no specific considerations and only neurotypical people were hired for the job. Furthermore, one of the interviewees also identified a few provisions, such as speech-to-text software for employees with vision-related disabilities, but those provisions are allowed as exceptions depending on the case.

Future directions

Furthermore, in line with the second objective—that is, to explore the



- There is a need for raising awareness on the topic of cognitive disabilities.
- Monetary concerns in this regard must be addressed.
- Development of newer version of standards that consider cognitive disabilities.
- Need for regulations, governmental directives.
- Improvement on organizations internal risk assessment procedures for considering diverse avenues such as this.

- Usability and accessibility of the products needs to improved.
- There needs to be a consideration when normally abled people have burnout which may also impact their decision-making abilities.

FIGURE 2. Avenues for the future concerning cognitive disabilities.

avenues for future research and practice for the inclusion of cognitive disabilities in the design and development of cybersecurity functions—the first- and second-order concepts and aggregated themes are presented in Figure 2.

Avenues for the future. Having identified this nonconsideration of cognitive disabilities in the design and development of cybersecurity functions in line with the objectives, the interviewees were asked about their opinion on how to improve the state of the art. The interviewees identified dimensions, such as raising awareness, taking initiatives from a financial perspective, legislation, and sanctions to improve the state of the art. Raising awareness would involve conducting seminars and workshops where security and other design and development personnel are briefed about the challenges faced by cognitively challenged users. Furthermore, policymakers can contribute to the improvement in the state of the art by introducing legislation that dictates such considerations in the development of cybersecurity functions.

Other considerations. It was revealed during the interviews that neurotypical users might face additional challenges while performing cybersecurity functions in a condition called *burnout*. Burnout causes a state of complete mental and physical exhaustion and cybersecurity-related decisions, such as detecting a phishing email or responding accurately to a security warning, which might be impacted when neurotypical employees or end-users are experiencing this state. Therefore, it is relevant to consider cognitive functions in relation to cybersecurity not just for users with disabilities, but also for neurotypical users experiencing burnout and exposed to increased threat due to reduced cognitive abilities during a certain period of time.

DISCUSSION

This article aims to review how cognitive disabilities in relation to cybersecurity are considered in practice. Briefly, the core result shows practitioners agree that cognitive disabilities are important to be considered in the development of cybersecurity functions; however, the extent to which they have been considered so far is limited.

Ten practitioners participated in the interviews and were asked about how their companies consider cognitive disabilities in the development of cybersecurity functions for customers and in their internal cybersecurity practices. The consensus was that cognitive disabilities were not considered in any of those aspects, except in a few cases where it has been specifically requested by someone. Most respondents said they never really thought

ABOUT THE AUTHORS

BILAL NAQVI is a postdoctoral researcher at Lappeenranta-Lahti University of Technology, 53850 Lappeenranta, Finland. His research interests include human aspects of security and security implications of digitalization schemes. Naqvi received a Ph.D. software engineering from Lappeenranta-Lahti University of Technology, Finland. He is a member of International Federation for Information Processing (IFIP) TC 11 Working Group 12 on Human Aspects of Information Security and Assurance, and IFIP Working Group 13.2 Methodology for User-Centered System Design. Contact him at syed.naqvi@lut.fi.

JOAKIM KÄVRESTAD is a senior lecturer in informatics at the Jönköping School of Engineering, 553 18 Jönköping, Sweden. His research interests include working within usable and equal access to security and how user abilities impact the ability to be secure. Kävrestad received a Ph.D. in in context-based microtraining-enhancing cybersecurity training for end-users. He is involved in the European Union Agency for Cybersecurity Ad Hoc Working Group on Awareness Raising. Contact him at joakim.kavrestad@ju.se.

A.K.M. NAJMUL ISLAM is a professor conducting research in responsible, trustworthy, and lawful digital system design and development using blockchain and artificial intelligence, and impacts of digital systems on individuals and organizations at Lappeenranta-Lahti University of Technology, 53850 Lappeenranta, Finland; an adjunct professor at Tampere University, 33100 Tampere, Finland; and senior editor for the journal *Information Technology & People*. Islam received a Ph.D. in information systems from the University of Turku, Finland. Contact him at najmul.islam@lut.fi.

about it, but that it was something they should probably address. The respondents further said that the topic had never been on their agenda but is important now that they know about it. They described that cybersecurity is governed by many different standards and legislation and consideration of cognitive disabilities is not needed for compliance with those, and therefore left in the dark. The interviewees further suggested that highlighting cognitive accessibility in governing laws and standards is probably needed for the industry to put an emphasis on it.

The findings revealed that cognitive disabilities are not considered while designing and developing cybersecurity functions and that several challenges hinder the inclusion of cognitive disabilities. Some of these challenges include: 1) lack of such requirements specified by the clients, 2) lack of legislation governing such inclusion, and 3) less market potential. Furthermore, it was also revealed from the perspective of the avenues for the future that raising awareness on the topic among different stakeholders could help incorporate cognitive disabilities in the design and development of cybersecurity functions. In addition, providing incentives to the industry in terms of monetary benefits could also provide a push toward such inclusion.

Cognitively accessible cybersecurity is important for users who suffer from cognitive disabilities. As discussed earlier, the cognitive ability of neurotypical users may be negatively impacted by temporary conditions, such as burnout. Even stress and weariness can cause a person's cognitive abilities to be temporarily lowered. Consequently, cognitively accessible cybersecurity functions can be beneficial for all users.

This research shows that cognitive accessibility is important for making all users able to use cybersecurity functions. However, it also shows that both industry and research are far from ready to address the topic of cognitively accessible cybersecurity. While explored research identifies that cognitive accessibility lowers the bar for the adoption of cybersecurity functions, practitioners suggest that laws and standards that the industry must comply with do not focus on this issue. A suggestion, considering this research, is that decision-makers and standardization bodies include cognitive accessibility into governing documents.

This research shows that cognitive accessibility is an important cybersecurity topic and reveals that both research and practitioner insight are scarce. Consequently, there are several avenues for further research. One such avenue would be to focus on the cognitive energy required to engage with cybersecurity functions. Being able to measure how much energy a certain tool or process requires would be beneficial and developing such a metric could be a direction for future work. Another possibility is to focus on the needs of the industry by researching the industry's preparedness to include cognitive accessibility in cybersecurity practices.

ACKNOWLEDGMENT

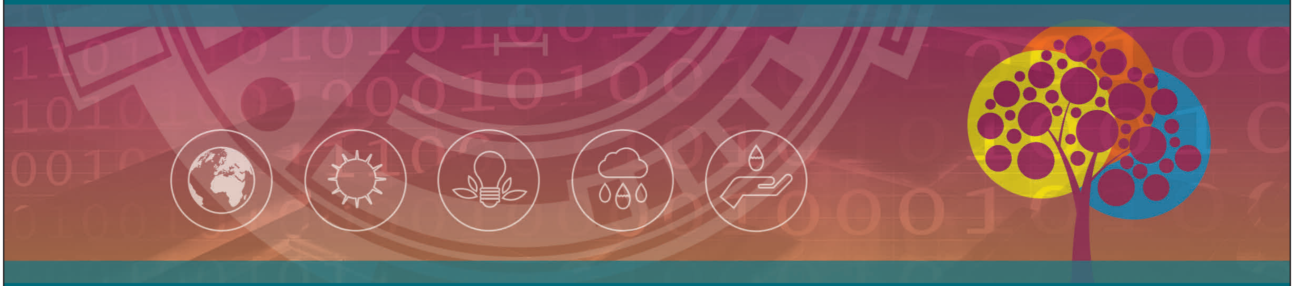
This work involved human subjects in its research. The authors confirm that all human subject research procedures and protocols are exempt from review board approval as per the Finnish national research regulations.

REFERENCES

1. "Disability." World Health Organization. Accessed: Oct. 9, 2023. [Online]. Available: https://www.who.int/news-room/fact-sheets/detail/disability-and-health
2. "Cognitive disabilities." FCC. Accessed: May 9, 2023. [Online]. Available: https://www.fcc.gov/cognitive-disabilities
3. "Disability impacts all of us." CDC. Accessed: May 9, 2023. [Online]. Available: https://www.cdc.gov/ncbddd/disabilityandhealth/infographic-disability-impacts-all.html
4. M. Karwowski and J. C. Kaufman, *The Creative Self: Effect of Beliefs, Self-Efficacy, Mindset, and Identity*. London, U.K.: Academic, 2017.
5. K. Oberauer, H.-M. Süß, R. Schulze, O. Wilhelm, and W. W. Wittmann, "Working memory capacity—Facets of a cognitive ability construct," *Personality Individual Differences*, vol. 29, no. 6, pp. 1017–1045, 2000, doi: 10.1016/S0191-8869(99)00251-2.
6. C. Robson and K. McCartan, *Real World Research*. Hoboken, NJ, USA: Wiley, 2016.
7. I. Etikan, S. A. Musa, and R. S. Alkassim, "Comparison of convenience sampling and purposive sampling," *Amer. J. Theor. Appl. Statist.*, vol. 5, no. 1, pp. 1–4, 2016, doi: 10.11648/j.ajtas.20160501.11.
8. "Sustainable development goals (SDGs) and disability." United Nations. Accessed: Oct. 9, 2023. [Online]. Available: https://social.desa.un.org/issues/disability/sustainable-development-goals-sdgs-and-disability
9. M. Belk, C. Fidas, P. Germanakos, and G. Samaras, "Do human cognitive differences in information processing affect preference and performance of CAPTCHA?" *Int. J. Human-Comput. Stud.*, vol. 84, pp. 1–18, Dec. 2015, doi: 10.1016/j.ijhcs.2015.07.002.
10. A. Vishwanath, B. Harrison, and Y. J. Ng, "Suspicion, cognition, and automaticity model of phishing susceptibility," *Commun. Res.*,

vol. 45, no. 8, pp. 1146–1166, 2018, doi: 10.1177/0093650215627483.

11. R. Gutzwiller, J. Dykstra, and B. Payne, “Gaps and opportunities in situational awareness for cybersecurity,” *Digit. Threats, Res. Pract.*, vol. 1, no. 3, pp. 1–6, 2020, doi: 10.1145/3384471.
12. M. W. Boyce, K. M. Duma, L. J. Hettinger, T. B. Malone, D. P. Wilson, and J. Lockett-Reynolds, “Human performance in cybersecurity: A research agenda,” in *Proc. Human Factors Ergonom. Soc. Annu. Meeting*, 2011, pp. 1115–1119.
13. L. Palmer, “The relationship between stress, fatigue, and cognitive functioning,” *College Student J.*, vol. 47, no. 2, pp. 312–325, 2013.
14. S. J. Verhagen et al., “Measuring within-day cognitive performance using the experience sampling method: A pilot study in a healthy population,” *PLoS One*, vol. 14, no. 12, 2019, Art. no. e0226409, doi: 10.1371/journal.pone.0226409.
15. L. Lundin et al., *Psykiska Funktionshinder: Stöd Och Hjälp Vid Kognitiva Funktinsnedsättningar*, 2nd ed. Lund, Sweden: Studentlitteratur, 2012.
16. D. A. Gioia, K. G. Corley, and A. L. Hamilton, “Seeking qualitative rigor in inductive research: Notes on the Gioia methodology,” *Org. Res. Methods*, vol. 16, no. 1, pp. 15–31, 2013, doi: 10.1177/1094428112452151.
17. M. Lamond, K. Renaud, L. Wood, and S. Prior, “SOK: Young children’s cybersecurity knowledge, skills and practice: A systematic literature review,” in *Proc. Eur. Symp. Usable Secur.*, 2022, pp. 14–27, doi: 10.1145/3549015.3554207.
18. J. Kävrestad, A. Hagberg, R. Roos, J. Rambusch, and M. Nohlberg, “Usable privacy and security from the perspective of cognitive abilities,” in *Proc. IFIP Int. Summer School Privacy Identity Manage.*, Cham, Switzerland: Springer International Publishing, 2021, pp. 105–121.
19. S. T. Marne, M. N. Al-Ameen, and M. K. Wright, “Learning system-assigned passwords: A preliminary study on the people with learning disabilities,” in *Proc. 13th Symp. Usable Privacy Secur. (SOUPS)*, 2017. Available at: https://www.usenix.org/system/files/conference/soups2017/wips2017-marne.pdf



Digital Object Identifier 10.1109/MC.2024.3397363