



Examination of cybersecurity in open and distance learning within the scope of technical support services

Sehla Ertan ^{a *} , T. Volkan Yüzer ^b 

^a Turkish-German University, Türkiye

^b Anadolu University, Türkiye

Suggested citation: Ertan, S. & Yüzer, T. V. (2024). Examination of cybersecurity in open and distance learning within the scope of technical support services. *Journal of Educational Technology & Online Learning*, 7(2), 254-272.

Highlights

- With nearly three centuries of institutional and theoretical history, open and distance learning (ODL) activities need to meet different expectations and needs in line with the increase in the adult learner population.
- Technical support services represent a holistic structure covering the technical and technological components of ODL systems.
- ODL systems generate, store and transfer large amounts of data. As one of the critical infrastructural elements, the ODL platform accommodates large audiences. All stakeholders involved in all of the processes in the system are in constant interaction with instructors, learners, content, technology and the system itself through online network structures.
- Cybersecurity, which is examined within the scope of technical support services, contains the limited nature of the human factor both as a system user and as a technical team member. Therefore, it may be useful to transform the factors that bound rationality in an industrial support structure into rational and mechanistic structures.

Abstract

Open and distance learning (ODL) activities aim to meet the expectations and needs of different individuals, societies, and systems by ensuring the continuation of learning with a lifelong learning philosophy and an egalitarian policy for everyone, regardless of time and place. Support services, which address the differentiated expectations and needs in all learning-related activities, serve the learning processes and the various stakeholders involved. Therefore, technical support services are included in support activities that require the use of technology as a tool, mediator, or technique in learning processes. In this study, ODL systems that are situated in digital space are examined within the scope of technical support services in line with the threats and dangers of the developing and expanding digital space. The aim is to create a technical support service model based on Herbert Simon's Bounded Rationality Theory and Otto Peters' Industrialization Theory, to ensure cybersecurity in ODL systems. In this study, which adopted a case study as one of the qualitative research methods, documents in the literature were examined first. Considering the literature, the opinions of eight field experts were gathered by ten interview questions. After the semi-structured interviews were transcribed, the data obtained were divided into codes and themes through thematic analysis. The findings stressed the importance of institutional culture, distribution of tasks and responsibilities, administrative support, institutional awareness, cybersecurity training, and the use of different technologies to ensure cybersecurity in ODL systems. Additionally, the experts emphasized a common view that smart systems should be used in the provision and maintenance of cybersecurity.

Article Info: Research Article

Keywords: *Open and distance learning, support services, technical support services, cybersecurity*

* Corresponding Author. Turkish-German University, Türkiye.
e-mail address: ertansehla@gmail.com

1. Introduction

Open and distance learning (ODL) systems provide innovative, equitable, and flexible learning opportunities, environments, and resources to large masses independent of time and space, through technology (Firat, 2020). Monitoring, improving, and updating the services provided in line with the expectations or needs of each stakeholder (e.g. learner, instructor, administration, staff, etc.) involved in the process are carried out within the scope of support services (Genç Kumtepe et al., 2019). In this respect, it is possible to see that support services, which play an important role in the functioning of ODL activities (El Turk & Cherney, 2016), are handled by different researchers with various classifications (Genç Kumtepe et al., 2019). However, it is important to examine ODL activities, which represent a technical and technological structuring by nature, from a framework that will cover all processes in the context of "technical support services" (Durak, 2017).

Technical support services represent a holistic structure covering the technical and technological components of ODL systems. The technical support structure, which consists of various layers such as *"infrastructure components"*, *"technology-based processes"*, *"communication and interaction elements"*, and *"software, hardware and network structures"*, also includes concerns and activities related to the security of data, individuals, processes and the system (Alexei & Alexei, 2021; Dhillon, 2020; Durak, 2017; El Turk & Cherney, 2016). Cybersecurity, which represents the protection of assets (data, individuals, technology, systems, institutions, or governments) that interact with information and communication technologies against all kinds of malicious attempts and manipulation, refers to precautions, foresight, and defense activities against security threats or breaches (Fischer, 2016; Jang-Jaccard & Nepal, 2014). ODL systems, which generate, store and transfer large amounts of data in the interaction environments they offer within a wide technological spectrum, have become a promising potential "open" target for cyber-attacks that diversify day by day.

Considering the critical processes that need to be managed in cybersecurity and the increasing amount of data, it is very difficult for active users and decision-makers in the system to overcome cyber-attack processes unless there is significant automation in the systems (Nespoliet al., 2018). At this point, it is necessary to employ smart systems to ensure cybersecurity. The study aims to create a technical support service model for the processes of preventing cyber-attacks against ODL systems and ensuring cybersecurity. To ensure cybersecurity in the support service structure, it is anticipated to use machine learning in line with Otto Peters' Industrialization Theory. This proposal is addressed in the context of the "Bounded Rationality Theory" of Herbert Simon, one of the leading figures in artificial intelligence. In line with the determined purpose, answers to the following questions were sought:

1. What are the limits and limitations of system stakeholders and technical support services in ensuring cybersecurity in ODL systems?
2. How can cybersecurity be ensured within the scope of the technical support services of ODL systems?

2. Literature

ODL systems, which offer a time and space independent learning experience through various communication and internet technologies, involve many stakeholders such as learners, instructors, administrators, and staff (Genç Kumtepe et al., 2019; Okur, 2012). With nearly three centuries of institutional and theoretical history, ODL activities need to meet different expectations and needs in line with the increase in the learner population. All activities that address relevant expectations and needs within the scope of ODL are examined under the heading of "support services".

It is seen that support activities, which started as "counseling services" based on the concept of face-to-face education, are shaped within the framework of "support services" day by day in line with the diversifying learner population, the use of different technologies in learning-teaching processes and diversified expectations (Brindley, 1987; Durak, 2017; Firat, 2016; Genç Kumtepe et al., 2019; Rekkedal, 1981; Sewart, 1980; Zawacki-Richter, 2004). Considering that applied ODL activities have a much longer

theoretical history than theoretical ones, there are also support structures that vary according to the context of these activities.

2.1. Technical Support Services in Open and Distance Learning

ODL systems are technological so technological issues are one of the critical factors that can prevent ODL stakeholders from benefiting from the system (Almaiah, Al-Khasawneh & Althunibat, 2020; Yumurtacı, 2020). Therefore, all technological components of the system and processes should be examined within the scope of technical support services. In this respect, it is possible to say that more than one stakeholder needs differentiated technical support activities within the scope of diversified learning-teaching processes. In this respect, the summary below captures the essence of the researchers' contribution to technical support services in educational environments.

Table 1.

Technical support services

Researcher(s)	Contributions to technical support services in educational environments
Keast (1997)	Provision and efficient operation of learning environments
Padgett & Conceicao-Runlee (2000)	Technical training to improve technology usage skills of teaching staff.
Lee (2003)	Technical support for learners via communication channels during working hours.
Muilenburg & Berge (2005)	Support activities for all technical problems and inadequacies.
Somayajulu & Ramakrishna (2008)	Learner support services including computer lab setup, program promotion, hosting, development, maintenance, network facilities etc.
Okur (2012)	Support services for teachers in technology-based activities like content production and delivery.
Khanna & Basak (2013)	Services for software and hardware installation, maintenance, infrastructure design, service delivery, and system evaluation.
Arko-Achemfuor (2017)	Focus on computer and internet access within learner support services.
Durak (2017)	Solutions to software, hardware, and network-based problems.
Roddy et al. (2017)	Development of technological competencies and capabilities.
Genç Kumtepe et al. (2019)	Support for learners and staff, including technical infrastructure information and improving lecturers' ICT use and teaching strategies.

Technical support has a positive impact on learners' motivation and retention in their learning process (Alshammari, 2020; Antwi-Boampong, 2021). Therefore, technological barriers and problems need to be overcome in order to carry out ODL processes efficiently. Technological issues are related to inconsistent learning platforms, browsers or software, which occur in the absence of technical support services and negatively impact learning processes (Muilenburg & Berge, 2005). Those problems also can disrupt both the teaching-learning process and the development of technical competencies (Gutiérrez-Santiuste, Gámiz-Sánchez & Gutiérrez-Pérez, 2015). Technical problems, which include hardware, software, or network problems, can be caused by inadequate infrastructure, technological failures, power outages, or disruption in internet access/speed (Durak, 2017; El Turk & Cherney, 2016).

ODL systems include learners, instructors, administrative staff, and most importantly a critical digital infrastructure where data is created and processed. Therefore, digital interaction in these systems has a multifaceted and comprehensive spread. Because these systems, where learning is open to people, place, time, ideas and methods, are by nature in interaction with their environment (Firat, 2021). ODL systems with low-security measures are therefore vulnerable to various attacks by attackers in different locations, roles or positions (Minh Hoang et al., 2020; Ulven & Wangen, 2021).

Security concerns, which are in close contact with technical problems such as "software and hardware failures", "network structures", "deviations in service quality", "technological obsolescence", "individuals' usage errors" or "their inability to use technology" (Alwi & Fan, 2010; Minh Hoang et al., 2020), directly concern ODL systems in line with the definitions above. For this reason, it is very important for ODL systems to ensure system security and continuity with a stable institutional structure against the dynamic challenges of cyberspace.

2.2. Cybersecurity

Globalization, which is shaped by digital dynamism and shapes digital dynamism, has transformed the tangible global order into a digital form and structured the perception of built-in tangible space as "dimensionless space" or "cyber-space" (Çiftçi & Karakuş, 2019, p.14). The term "cyberspace", first used by the Canadian writer William Gibson (1984) in his science fiction novel *Neuromancer* to describe the structure and scope of the Internet, represents the aforementioned structuring. The digitalization of technological assets, their inclusion in the network structure, and their transformation into communication tools that provide data flow (information and communication technologies) create the constantly developing cyberspace. This continuous evolution also diversifies the threat environments and applications in cyberspace, expanding the scope of potential attacks (Jang-Jaccard & Nepal, 2014; Ulven & Wangen, 2021).

Cybersecurity, which is the terminological equivalent of precaution and defense processes in cyberspace, refers to the environment where digital attacks and criminal activities take place, refers to protecting data, individuals, networks, devices, programs, systems, institutions, and governments against various attacks (Fischer, 2016; Minh Hoang et al., 2020). Assest whose confidentiality, integrity, and accessibility are protected in cyberspace with protection activities are safe.

Cyberspace, which increasingly encompasses the life and interaction elements of the digitalized global order, not only creates a profitable market for the execution of criminal elements but also minimizes the risk of criminals being caught. In this respect, the fact that attacks in cyberspace, which represent infinite geography without physical borders, are carried out by anonymous attackers makes it difficult to track and detect these attacks. In addition, the fact that the minimum requirement to carry out an attack is a computer and a network connection makes cyberattacks attractive and profitable due to their low cost (Jang-Jaccard & Nepal, 2014). However, cyber-attacks can be diversified according to the attacker's approach and purpose. These attacks, which target different sectors, directly affect the field of ODL, where digital tools and network technologies are used extensively.

2.3. Cybersecurity in Open and Distance Learning Environments

Online learning applications and platforms, which represent a modern form of education within the framework of ODL practices, are systems that generate, store and transfer large amounts of data. As one of the critical infrastructural elements, the ODL platform accommodates large audiences. All stakeholders involved in all of the processes in the system are in constant interaction with instructors, learners, content, technology and the system itself through online network structures. These inherently open platforms are a rich source of data, with elements and vulnerabilities that can be easily accessed for digital attacks and exploitation. These platforms, which are open in nature, are a very rich data sources with elements and vulnerabilities that can be easily accessed for digital attacks and exploits (Udroiu, 2017).

The use of computer and internet technologies in learning-teaching processes and the inclusion of multidirectional interaction channels in the process bring disadvantageous scenarios by turning into some security weaknesses (Bandara, Ioras & Maher, 2014; Udroiu, 2017). Therefore, protecting the confidentiality, integrity, and availability of data is crucial to keep learners and learning processes safe.

In ensuring and maintaining cybersecurity in ODL systems, all stakeholders in the system should make some decisions in the stages of predicting, detecting, preventing or defending cyber-attacks. These decisions may involve decision processes to distinguish whether a digital action or content is a cyber-attack, or they may refer to decisions to design and execute processes to actively detect, prevent, or defend against attack activities.

The technical measures taken to ensure and maintain cybersecurity have an important role in ensuring the prestige, durability, and continuity of an institution. This situation indicates that an ideal cybersecurity system and culture should be created from a technical perspective within the framework of institutional structuring. Similarly, ODL systems need a coherent structure with technical hardware, software, and

networks to create an infrastructure that ensures the sustainability of learning activities, and experts to support this structure (Gümüş, 2020).

Considering the critical processes that need to be managed in cybersecurity and the increasing amount of data, it is very difficult for active users and decision-makers in the system to overcome cyber-attack processes unless there is significant automation in the systems (Nespoli et al., 2018). At this point, it is necessary to employ smart systems in cybersecurity.

Simon (1955), with his "Bounded Rationality Theory", emphasized that the human brain's computational ability is bounded and that there may be uncertainties and information deficiencies in the preference and decision stages. In this direction, Simon (1955; 1976) stated that people who play a leading role in decision-making cannot make realistic and logical, in other words, rational decisions due to many limitations due to their cognitive nature. He defined the factors bounding rationality as "bounded information", "bounded evaluation", "bounded decision-making ability", "bounded ability" and "boundless uncertainty" (Simon, 1972).

Bounded rationality in cybersecurity management, which includes an organizational management policy, can be overcome with Otto Peters' Industrialization Theory. This theory discusses many components of industrial production, such as the rationalization, mechanization, planning, and organization of organizational processes in distance education by experts in units. With this theory, which discusses many industrial production components such as rationalization, mechanization, planning, and organization of organizational processes in distance education by experts in units (Peters, 1993; 2010), an industrial approach can be adopted in ensuring cybersecurity in ODL institutions.

Considering the information given, the use of smart systems is seen as an approach worth examining in order to make fully rational decisions in ensuring cybersecurity, which is under the problems experienced in technical support services in ODL systems. From this point of view, the technical support provided in ODL systems should be supported by advanced technologies such as artificial intelligence and machine learning as well as manpower. Accordingly, this study aims to create a technical support service proposal using machine learning in cybersecurity based on Bounded Rationality and Industrialization Theories in order to actively or passively prevent cyber-attacks against ODL systems and their stakeholders and to ensure cybersecurity.

3. Methodology

In this study a case study as one of the qualitative research approaches was adopted. The case study allows the issue or problem of interest to be considered as a whole and allows this situation to be examined in detail (Thomas, 2021). In the design and planning of case studies, it is possible to talk about 3 basic stages. These are respectively "defining the situation", "determining the case study design" and "placing the case study in a theoretical framework" (Yin, 2017). The following table can be taken as a reference in the design determination phase in case studies.

The case studied in this paper is what new, automated, and rational approaches can be taken to ensure the security of ODL systems considering studies and expert views on cyber security activities in those systems. Therefore, a holistic single-case design was adopted. In holistic case studies with a single unit of analysis, the presence of at least one of three different situations necessitates the use of this design (Yıldırım & Şimşek, 2013). The first is situations that necessitate the use of this pattern to confirm or refute a well-formulated theory. In this study, a technical support service model has been validated within the framework of Otto Peters' Industrialization Theory, based on the Bounded Rationality Theory, which argues that human cognition is limited, in order to ensure cyber security in ODL systems.

The study of unique, contradictory or extreme situations is the second sign that this pattern should be used (Yıldırım & Şimşek, 2013). The last one shows that this design needs to be used in examining a situation that has not been studied or reached before. In line with the literature review conducted in this context, it has been seen that there is no adequate and unique model to ensure cybersecurity within the scope of technical support services. In this direction, the reason for using the holistic single-case design in this study,

which aims to investigate an additional situation, is that there is no access to studies on cybersecurity in the field of ODL.

3.1. Data Collection and Analysis

Within the scope of the study, data were obtained through literature analysis and semi-structured interviews. As a result of the document review conducted to support the theoretical framework that shaped the study with the studies in the literature, interview questions that reflect and feed the theoretical framework were created.

3.2. Participants

Qualitative research approaches aim to examine a central phenomenon, situation or concept in depth, rather than generalizing research findings to a specific population (Creswell, 2013). In research conducted for this purpose, different participants may need to be involved in the research processes in understanding, interpreting, defining and evaluating the central phenomenon. Within the scope of the determined framework, it is possible to include the participants who will be involved in the research process in the relevant process with probabilistic and non-probabilistic approaches. In qualitative research approaches that do not seek to represent the universe, it is seen that the participants included in the process are included in the research in line with the non-probability sampling method (Creswell, 2013). Within the scope of this research, the "purposive sampling" approach, one of the non-probability sampling methods, was adopted.

Participants selected through purposive sampling were included in the process, considering that the views on the situation examined within the framework of the purpose of the research could be addressed in the natural flow of the research. It is important to select the data sources (participant, environment, event, or data) that will be included in the process in a way that best supports the research subject in order to be able to make definitions for the subject under research, describe the situations and eliminate problematic situations. In this direction, the experts included in the research were included in the process with the criterion approach from purposeful sampling methods. The participants included in the process with the criterion approach were selected based on the criteria mentioned below. These criteria can be shaped according to the purpose and scope of the research and the approach of the researcher (Yıldırım & Şimşek, 2013).

In this study, which was shaped by expert opinions in line with the research purpose and scope, the experts included in the process are national and international researchers with at least 10 years of experience in the fields of "open and distance learning", "support services in open and distance learning", "educational technologies" or "cybersecurity". These experts were also selected among researchers working in ODL institutions or units. Considering their inclination and experience in technical issues, the experts included in the study were researchers with advanced technology use and studies in the field of learning with technology. Considering that at least 4-5 participants should be included in the process in case studies (Creswell, 2013), the research process was shaped with 8 experts. Demographic information of the participants is presented in Table 3.

Table 3.

Participant list

Nicknames	Institution	Experience	Field
P1	The Open University	40 years	support services in open and distance learning
P2	Anadolu University	20 years	Educational technologies
P3	Ataturk University	19 years	Open and distance learning
P4	Eskisehir Technical University	18 years	Cyberseucurity
P5	Anadolu University	15 years	Open and distance learning
P6	Balikesir University	13 years	Educational technology
P7	Anadolu University	12 years	Cyberseucirty & ODL
P8	Anadolu University	11 years	Open and Distance learning

3.3. Data Collection Tools and Obtaining Data

In this study, data were collected through document analysis and interviews. Semi-structured interview structure was adopted among the interview methods that vary as structured, semi-structured and unstructured (Fraenkel, Wallen & Hyun, 2012). Semi-structured interviews, which allow open-ended questions reflecting the scope and purpose of the research to reflect the views and experiences of the participants within a certain framework, help the data collection process to progress under the control of the researcher by providing a more flexible environment. In addition, it is possible to state that this technique provides a more flexible and easy structure for organizing and analyzing the data as well as obtaining them easily. In this direction, the interview questions were structured in a way to be based on the Bounded Rationality and Industrialization Theories. The relevant interview questions are given in Appendix 1.

The interview questions were based on the data obtained from the document analysis. In this process, firstly, written permissions were obtained from the experts via e-mail regarding their participation and the recording of the interviews; accordingly, interview dates and times were determined. The data were collected with the participation of 8 different experts: 3 face-to-face, 2 online, 2 in writing, and 1 by phone. Afterward, the data recorded in 3 different forms as video, audio, and written were analyzed.

3.4. Data Analysis

Firstly, the data was recorded in audio, and both video and audio forms were transcribed by the researcher. The transcribed data and the data obtained directly in writing during the data collection process were transferred to the NVivo package program. Afterwards, codes and themes were created.

The data collected through semi-structured interviews were analyzed using content analysis. Content analysis, which allows the data obtained from different types of sources for the situation to be examined with an inductive approach, makes it possible to examine, classify, evaluate, associate, describe, and interpret different dimensions of situations in depth (Fraenkel, Wallen & Hyun, 2012). The transcribed data were first read from beginning to end, and then, considering the general structure of these data, codes, and themes related to the interview questions were extracted from the data texts. The findings were described and interpreted in a way to answer the main questions and problems of the research.

3.5. Research Reliability

Codes and themes were created by analyzing the interview data. The codes and themes generated by content analysis were checked by three independent researchers. In order to ensure the reliability of the research by providing these analyses, the compatibility of the relevant results was compared. This comparison was based on Miles and Huberman's (1994) formula " $\text{Agreement} / (\text{Agreement} + \text{Disagreement}) \times 100$ ". The result obtained according to this formula showed that the reliability between the researchers was 90%.

4. Findings

The findings reveal that ODL systems are vulnerable targets for cyber-attacks due to the openness policy adopted by ODL systems and the large number of stakeholders with different roles. The findings, which emphasize the importance of system structuring as a priority in cybersecurity activities, indicate that communication and coordination between units of ODL systems are critical to ensure security.

"...cyberspace is very vast. Attacks can have many reasons and you cannot understand where they originate from. Therefore, the parts of that system must be compatible with each other. In other words, the network unit and the system unit, and the server management unit must be compatible. That organization and coordination must be very good..." P3

"...Limitation is a feature that comes from the boundaries of human nature. Human beings have limited cognitive capacity, human beings have limited decision-making mechanisms. If there is a human factor in a system, it is always necessary to consider variability, support, lack, or limitation, and at the same time it

requires diversity. In order to support this boundary, the coordination of teams and the system is expected to support coordination with the data it receives from all these teams...” P5

The findings point out that cybersecurity activities, which are covered under technical support services, do not only concern the technical team, indicate that separate units should be established for cybersecurity activities in ODL systems. Therefore, cybersecurity activities in ODL systems should be supported by a structure that includes the technical team.

“...It may not be economical to have a sufficient number and quality of technical support service personnel in a localized environment. The creation of a centralized structure or structures divided into regions according to infrastructure / needs / preferences can ensure that healthy and effective decisions can be delivered quickly to more stakeholders...” P2

“...There are no people completely dedicated to cybersecurity in the units. Generally, it feels like an additional task for the people who look after the system unit or the network. An individual cyber-attack prevention unit should be established. People with different tasks should be brought together. It is important to employ such personnel and human resources...” P3

“...security experts are very important in this process. So, the human factor is very important here. I feel that the establishment of security units as separate units is the least important issue, especially in our field...” P7

The data shows that since the technical support team is not kept separate from the cybersecurity team. The findings supported that another boundary between the stakeholders and the technical team in the system is their limited cognitive capacity. Accordingly, the lack of necessary and sufficient cybersecurity awareness of both the system stakeholders and the technical team, the lack of training for the technical team on these activities, the lack of a corporate cybersecurity culture, the lack of structuring the distribution of roles and responsibilities in security activities, and the fact that all these are not handled under managerial support are defined as limits and boundaries.

“...technical support team should not be alone. The technical support team may only deal with the technical side of the business, but cybersecurity is not only about technical support. It is the training of people, the communication of stakeholders, the mutual awareness of stakeholders... The management organization should be organized in a structure that does not exclude this technical support team...” P5

“...Such specialists could be trained in emerging technological systems. They could be trained in the working structure of systems, and perhaps in meta-analysis, and then only be involved in some aspects of decision-making...” P6

“...Extra in-service training can be provided to people with limited assessment skills. They can be sent to trainings in national and international in order to further increase their evaluation skills and to know which attacks are aimed at what...” P7

“...I think it is important to consider that your technical support team is also students. All of them need to be approached as students in terms of security. They are constantly learning. I mean, they need to learn...” P1

“...security certificates such as the CEH (Certified Ethical Hacker) certificate can be obtained to specialize in attack prevention and defense activities. Because we are as strong as the weakest link in cybersecurity. One of the weakest links in cybersecurity is the human factor...” P8

In the data obtained, it was suggested that an information mechanism should be used that stakeholders in the system should benefit from. It has been argued that this mechanism should be a learning mechanism and create awareness and foresight in ensuring cybersecurity.

“...It is necessary to set up such systems on-demand as a portal, an interface and keep it updated. Cyber-attacks need to be explained especially in user language. We do not expect much technical skill from learners and instructors in this sense. Therefore, it is necessary to build a mechanism where the types of attacks are explained and where they can get answers when they ask questions...” P3

“...It may be advisable to bring together personnel with similar roles and responsibilities in a dynamic electronic performance and sharing system that constantly updates itself. In this way, it may be possible to take early precautionary and training steps against new risks...” P2

“...Instant information is very important in cyber incidents. Therefore, an instant information mechanism needs to be established. It is heard quickly through different channels, before the incident takes place, through various things. That information mechanism needs to be well-designed. Accordingly, the necessary structuring, necessary measures or the necessary offensive must be taken...” P3

In this direction, it was emphasized to create a corporate memory and to strengthen it with a structure that interacts with different institutions. It has also been observed that it is important that the institutional memory and inter-organizational cooperation to be created also represent a cybersecurity culture. These activities can be considered to represent a social dimension to ensure cybersecurity.

“...First of all, the institutional memory is very important here. Corporate memory alone is not enough, it needs to be expanded (...). Road maps, decision trees, and flow diagrams of what can be done in case of an attack can be drawn. (...) What can be done before a cyber-attack? I think it can be done by analyzing past cases...” P3

“...There may be a need for dynamic sharing and performance support systems where competent stakeholders can mentor stakeholders with limited experience. It may also be advisable to share new experiences with stakeholders who may have similar problems, discuss solutions, and share the results and implications of tested actions at short intervals...” P2

“...What kind of attacks can occur in an open and distance learning system? First of all, we need to identify this. That is to say, to make a workflow, to make a list of this... (...). It is necessary to make a preliminary study of all of these, which measures can be activated in these attacks, and the biggest problem is to be caught unprepared...” P7

“...Very different problems can arise, sometimes from a side you never expected. Therefore, in order for the person to be able to see those anomalies (...) the know-how or the memory of that institution is very valuable. Therefore, we bring the two together here. In other words, it can be a structuring that will both use the data in the mechanics of the system and transform the experience of the user from the institutional memory into an evidence-based structure that machines cannot predict...” P3

“...I would say that universities should cooperate in learning from each other. I think there is already a lot of exchange of practices between universities on security issues, and in fact I am sure of that. But this needs to be strengthened. So that universities can respond not only in individual institutions but also in a group...” P1

The findings draw attention to the importance of utilizing smart systems, artificial intelligence, and machine learning approaches in addition to intra-organizational, inter-organizational, and expert support/training to support the limited nature of individuals involved in cybersecurity activities. In the data analyzed in line with the interview questions, it was seen that experts mostly emphasized the necessity of smart systems.

“...Considering the limited computational ability of the human brain, the concept of machine learning can be utilized with various artificial intelligence applications. With the developing technology, it can be assumed that such systems will increase and improve in terms of quality...” P6

“...Intrusion detection systems and intrusion prevention systems have been developed to protect technical support services information systems against external attacks. In terms of mechanization of technical support

services, the use of machine learning, deep learning, and artificial intelligence algorithms in intrusion detection systems is a good method for faster and more accurate detection of attacks...” P8

“...Especially the emergence of big data, the widespread use of digital technologies, and the abundance of such data in open and distance learning or large education systems increase the limitations of the individual even more. In other words, it becomes very difficult for a person or a team to have all the data. Where does that lead us? It leads to machine learning. It leads to databases where big data will be kept. These databases need to create a recommendation system with natural language processing, algorithms, and give the team information about what to do. Even more, if it can be done, it can turn into a structure where artificial intelligence extracts the emerging risks from big data and directly applies and transfers them to the system itself...” P5

“...By utilizing today's popular technologies such as artificial intelligence, machine learning and deep learning, errors caused by human factors can be avoided as much as possible. The use of such technologies in technical support services will also be important for organizations with a lack of technical personnel in terms of workforce evaluation...” P6

“...Here, attack and precaution must be matched. Think like an alarm system. For example, an earthquake cannot be known much in advance, but you can understand it thirty seconds before. As soon as the first attack comes, technical personnel should be activated immediately. We cannot solve this only with technical support specialists. For example, in the event of an attack, the firewall must be activated immediately with automated systems and stop the attack. It should even shut down the system if it needs to shut down the system...” P7

“...Unless a continuously learning and self-improving structure is created in which simple tasks are mechanized, local steps such as continuous infrastructure updates, staff reinforcement, hiring the best personnel, providing continuous technical support and formative evaluation will be quite tiring and impractical...” P2

“...The technical team has its own cognitive limitation, and the digital technology that will overcome this cognitive limitation will benefit from autonomous systems, that is, artificial intelligence, and natural language processing models. Like, GPT-3 for example...” P5

“... think that studies on industrial theory, which is one of the basic theories of distance education, have been carried out so far mostly on content production and mechanization of these contents. However, in the field of technical support services, this theory can be used in a similar way and technical support services packages with a certain extension can be created. According to their security needs, distance education units can choose the ones they need from these packages. Such kind of package systems that can be developed independently of the LMS or the platform used may become widespread in the future...” P6

“...artificial intelligence systems that will support the technical support team should be developed and reliable systems that are valid not only by this team but also at the international level should be developed and put into the service of this team...” P5

In the findings representing the academic dimension, it was stated that it is important to hire trained and qualified personnel in the creation of machine learning algorithms and mechanisms to be used to ensure cybersecurity. At the same time, it was emphasized that the people who will operate in this context should be people who have received cybersecurity training.

“...technical support specialists may need to be informed and trained on such intelligent systems that have emerged with the developing technology. Considering the limited computational capability of the human brain, they can be trained to perform meta-analyses based on the analyses made by such intelligent systems within the scope of support services. Or they can be trained to interpret and implement these analyses...” P6

“...What the technical team will do is not to sit in front of the computer and see the risks and intervene in the risks, but to develop the programs and protocols of computers that can see and intervene in the risks and are exempt from human limitations. This is the most logical thing we can do right now...” P5

5. Discussion and Conclusion

Since ODL activities have timewise, spatial, and transactional distance elements, learning processes should be supported with different service structures (Roddy et al., 2017; Tuquero, 2011). This structure, called support services, is addressed with many different definitions and classifications in line with the changing needs and expectations of different stakeholders (Genç Kumtepe et al., 2019). Moreover, while support structures generally involve different stakeholders, either learners or teachers, technical support services involve all stakeholders and the system itself (Alshammari, 2020). Therefore, it is possible to consider cybersecurity activities that concern and affect all stakeholders and the system itself within the scope of technical support services. Considering the technical and technological structure of the system, related needs and expectations represent a hierarchical process. At this point, Maslow's pyramid of needs can be adapted to ODL as follows.

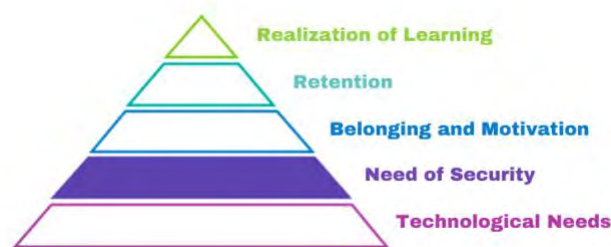


Fig. 1. Adaptation of Maslow's hierarchy of needs to ODL

It is possible to say that the ODL atmosphere, which is shaped by the use of technology and requires the use of technology, generally covers the actions performed in the digital world. However, with the use of technology, the digital world, which is a virtual manifestation of the real world, has turned into a cyberspace where various crimes and attacks targeting individuals, institutions, and governments take place day by day (Alexei, 2021; Fischer, 2016). ODL systems, which bring together various stakeholders from different parts of the world under the roof of a system through different technologies, have become a highly vulnerable and exploitable target for cyber-attacks (Alexie & Alexie, 2021; Bandara, Ioras & Maher, 2014). The findings obtained show that ODL systems operating in cyberspace where there is boundless uncertainty are directly affected by cyber-attacks and will continue to be affected.

According to the findings, past experiences in cybersecurity and organizational cybersecurity culture play an important role in diversifying security activities. The creation of a cybersecurity culture, which is an important part of information culture, will ensure the integrity of modern society and modern education elements. Creating a cybersecurity culture in an institutional context refers to a formation process in which institutional measures are taken in addition to technical measures (Reegård, Blackett, & Katta, 2019). Although the creation of a cybersecurity culture involves the training of technical staff, units, or structures, it is possible to say that it does not only cover this.

It is very important that individuals, units, systems, institutions, and states are aware of certain responsibilities to ensure cybersecurity and that they assume these responsibilities as a cultural element (Malyuk & Miloslavskaya, 2016). Reegård, Blackett & Katta (2019) argued that "management support", "cybersecurity policy", "cybersecurity awareness and training", "engagement and communication", and "learning from experience" components should be included in the system structure to create a cybersecurity culture. In line with the findings, the components that feed the institutional cybersecurity culture, respectively:

- Building communities of knowledge, practice and security,
- Establish communication and information mechanisms,

- Utilizing past learning and experience,
- Establishing networking and cooperation between individuals and units,
- Structuring role and responsibility definitions,
- Establishing administrative support, and
- Providing training and awareness-raising activities

At this point, technical, technological, administrative, academic, and social decisions should be taken and services should be provided in this direction in order to create an institutional culture. To create a cybersecurity culture in ODL systems, a support structure can be structured by considering these services. It is thought that structuring the activities that should be examined within the scope of technical support service in ensuring cybersecurity in a way that covers the entire system is important in ensuring system security as well as continuity.

It is important to train both system stakeholders and the technical support team in cybersecurity awareness and in line with their role definitions. Establishing information-based systems, ensuring that these systems have a structure that responds instantly to queries, continuously updating them, and creating an institutional memory by feeding them with past data will be useful in shaping current and future cybersecurity activities. In this direction, to create "security communities" by considering communities of practice, information, and knowledge.

It is considered important to examine all structures and processes that will ensure security in ODL systems. At this point, it is seen that the primary actor in ensuring cybersecurity is human (Bone, 2016; Chowdhury, Adam & Teubner, 2020). According to Simon (1976), human beings have boundaries that prevent them from making rational decisions. According to Simon's Bounded Rationality Theory, it is argued that individuals' rational decision-making and evaluation abilities can be handled within a bounded framework within the scope of boundless uncertainty. It is also supported by the findings of the research that these limitations stem from the cognitive nature of human beings as social beings and that the human factor brings with it limitations, uncertainty, and variability due to its nature. It is possible to encounter a similar situation when it comes to ensuring cybersecurity. Both the literature (Alferidah & Jhanjhi, 2020; Bone, 2016; Chowdhury, Adam & Teubner, 2020) and research findings indicate that cyberspace refers to a virtual world with boundless uncertainty and in this context, ODL systems are directly affected by this situation.

It is supported by the findings that ODL systems, which carry out learning-teaching activities in cyberspace, face boundless uncertainty in cybersecurity planning and practices. Individual judgment, decision-making, and competencies determine the fate of cybersecurity in anticipating, preventing, and defending against risks and attacks in the context of boundless uncertainty (Bone, 2016). Within the scope of Bounded Rationality Theory, the factors that put cybersecurity at risk in ODL systems can be listed as follows:

- Bounded information,
- Bounded capability,
- Bounded ability to evaluate,
- Bounded decision-making ability, and
- Boundless uncertainty in cyberspace.

At this point, bounded knowledge argues that not all information about a topic can be cognitively acquired, while bounded ability suggests that bounded action will occur despite the necessary competencies and competencies (Bone, 2016; Li, 2018). Similarly, in the processes of making individual and organizational decisions and evaluating these decisions, processes or outputs, there is bounded knowledge, bounded ability, and bounded evaluation in line with boundless options (Bone, 2016; Zhang et al., 2021). The findings show that these 5 factors directly affect each other. Therefore, in line with the findings, it is possible to mention the following boundaries in ensuring cybersecurity in ODL systems.

- Not having enough information to recognize the attack/threat or what to do in defense activities,

- Failure to assess how an attack will affect the system and its components,
- Inability to decide on a defense against risk or attack,
- Not having the competence and ability to take the necessary action concerning a decision,
- Failure to access the right information, make the right assessment, make the right decision, and apply the right method among boundless options.

Individuals with different job descriptions in all processes in ensuring cybersecurity in ODL cover all stakeholders in the system. It is possible to argue that each of these stakeholders, representing an institutional community within the framework of a security culture, plays a role in cybersecurity activities. Because naming and structuring cybersecurity only as knowing technology or having a technical team would be a very wrong and dangerous defense strategy (Dhillon, 2020; Li, 2018). Therefore, all stakeholders of ODL, including learners, instructors, administrators, and staff, each with a limited cognitive nature, have a place and responsibilities in differentiating cybersecurity activities.

Individuals in a system can play a role in ensuring cybersecurity, but they can also be the source of cyber-attacks or vulnerabilities that cause attacks (Dhillon, 2020; Fischer, 2016). This indicates that cybersecurity can be jeopardized by sources outside the system as well as by users within the system. The IBM (2021) reports that 95% of cyber-attacks are user-driven. In this direction, it is supported by the findings obtained within the scope of the research that it is important to raise awareness and train all stakeholders in the system about cybersecurity. When considered within the context of ODL systems, these individuals can be learners, instructors, or administrators, as well as technical staff responsible for technical and technological services under the umbrella of personnel. Considering the bounded cognitive nature of the system stakeholders and technical support team in the processes of ensuring cybersecurity in ODL, it is thought that the use of a mechanical structure relatively free of human factors to ensure the security of these individuals will create a more rational and secure system.

Otto Peters' (1993: 2000) Industrialization Theory suggests that the industrialization of ODL, starting with the letter and continuing with current internet technologies, does not directly represent the industrialization of education, but an industrial view of the production, distribution and use of education-related activities, contents and processes in learning processes. Technical support services, which serve within the scope of the technical and technological structure of emerging ODL systems, directly affect the production, distribution, continuity, and sustainability of educational activities, processes and contents (Firat, 2020; Yumurtacı, 2020). Therefore, the structuring of technical support services in an industrial format is important and necessary both for the system to be compatible with the units in industrial form and for the “rational” and “mechanical” structuring of cybersecurity.

The findings of the research support that cybersecurity, which is examined within the scope of technical support services, contains the limited nature of the human factor both as a system user and as a technical team member. Therefore, it may be useful to transform the factors that bound rationality in an industrial support structure into rational and mechanistic structures. In this direction, it is seen that the common suggestion that comes to the fore in the findings obtained within the scope of the research is the use of smart systems.

Traditional cybersecurity requires the implementation of static control mechanisms such as firewalls, intrusion detection systems, and intrusion prevention systems that monitor the hardware, software, and network structures of systems to implement security protocols within the framework of specific strategies and rules (Li, 2018). However, these passive defense methods and approaches alone are insufficient to create effective, and rapid responses to new cyber threats in cyberspace, which are increasingly expanding, uncertain, and aggressive due to the rapid increase in the use of digital technologies and big data (Zhang et al., 2021).

The findings of the research indicate that data-driven smart systems should play a role in security activities to ensure and maintain the security of ODL. In order to respond to cyber-attacks or to be strong against cyber-attacks and to implement protection of systems, the system needs to obtain historical and current

security status data and make intelligent decisions that can provide adaptive security management and control (Li, 2018). The findings indicate that artificial intelligence approaches such as machine learning, deep learning and natural language processing can be used in support service structures. Based on the findings of Fırat (2020), who stated that natural language processing technologies from intelligent systems can be used in learner support with a similar approach, it is supported by the findings obtained within the scope of the research that these technologies can also be used in technical support services in general and in ensuring cybersecurity in ODL systems. In line with the findings, a model for the structure of technical support services as follows.

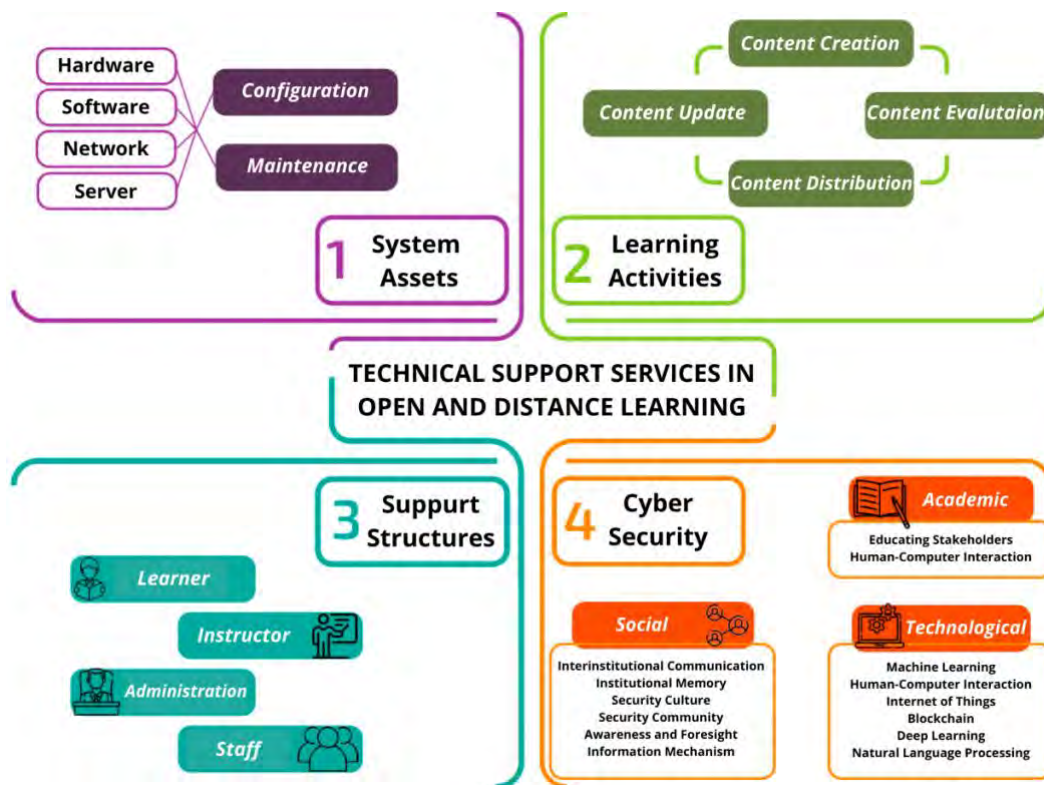


Fig. 2. A technical support service model in open and distance learning

The technical support service model in the figure above consists of 4 basic components. The first of these components, "system assets", covers the support of system assets that nurture and sustain technological readiness in ODL. It is envisaged that the installation of the system assets required for the realization of ODL activities and ensuring the sustainability of these assets and technical support services will be provided through this component. In the realization and execution of learning activities, the technical support service component, which is thought to be structured regarding the contents and the management of the contents, can be considered within the scope of "learning activities". In this context, various contents serving different purposes in line with different needs can be handled by different individuals and units in both academic and technical contexts. The production, evaluation, distribution, and updating of content can be sustained in this context.

The use of technology as a prerequisite for learning activities in open and distance learning systems, which represent a technical and technological structuring, can include different services that support technology and are supported by technology. The findings support that these services cover all stakeholders in the system: learners, instructors, staff, and administrators. Therefore, it is considered important to build technical support services as an umbrella support structure. Although it is possible to say that there are different support structures shaped according to institutional cultures and approaches, the technical support service model in ODL activities carried out in this direction should cover all different stakeholders in general.

In this model cybersecurity, the last component within the scope of technical support services, directly concerns the assets, individuals, and the system itself. Therefore, it has been observed that security activities

should be prioritized in all ODL activities where technological techniques are involved in learning processes. This component, which is analyzed under technical support services, can be analyzed under three main headings: academic, social, and technological. The document reviews and interviews conducted within the scope of the research support this approach. In this direction, training individuals who play a role in ODL activities and technical support services, creating institutional awareness, and ensuring human-computer interaction in all these activities cover the academic dimension of ensuring cybersecurity. At the same time, the technical team that will play a role in industrialization in ensuring the security of the system should be able to code smart systems and do so within the framework of cybersecurity, which points to the necessity of these activities.

The findings showed that within the scope of cybersecurity, it is necessary to create institutional memory, ensure communication and coordination between units, create a security culture, create security communities, and establish information mechanisms. Also, the findings of the research, which foresee the need for intelligent systems using machine learning in these mechanisms, show that awareness and foresight activities should be taken into consideration in these activities and that different institutions should be in communication. Therefore, it is thought that the social dimension in ensuring security is important in the system structuring to be shaped within the framework of cybersecurity.

The technological dimension, which is fed by both academic and social dimensions in order to ensure cybersecurity in ODL systems, covers the technical and technological structuring in learning activities. In addition to the components given in the related dimensions, the use of machine learning, deep learning models, and natural language processing technologies by considering human-computer interaction in this dimension, which includes the use of different techniques and technologies in ensuring cybersecurity, is supported by the research findings. In line with the findings predicting the transformation of cognitive rationality into an industrialized service structure in ensuring cybersecurity, academic, social, and technological dimensions feed each other in security activities.

In the findings representing the academic dimension, it was stated that it is important to hire trained and qualified personnel in the creation of machine learning algorithms and mechanisms to be used to ensure cybersecurity. At the same time, it was emphasized that the people who will operate in this context should be people who have received cybersecurity training. In line with the findings, machine learning should support the limited nature of individuals playing a role in cybersecurity activities; however, in order to create this support structure, qualified individuals should be included in the process. Therefore, it is seen that human-computer interaction should be taken into consideration at this point. This dimension can be considered to have both a technical and academic scope.

As a result, in line with the findings, it is recommended that security activities should be placed based on the system structure in order to ensure the realization and sustainability of ODL activities. Considering the place and importance of technical and technological processes in learning activities and Maslow's hierarchy adapted to ODL, it is thought that system structures should be shaped by prioritizing security concerns. At the same time, for ODL activities to be carried out safely, the technical and technological aspects of cybersecurity as well as its academic and social dimensions should be taken into consideration. Considering that the cybersecurity culture will be shaped within the framework of institutional culture in implementation-oriented activities, it should not be forgotten that the system-based security approach will constitute a whole that should offer individual and unit-oriented solutions.

Acknowledgement

This article was produced from a master's thesis at Anadolu University Social Sciences Institute.

References

Alexei, A. (2021). Cyber security strategies for higher education institutions. *Journal of Engineering Science*, 2021(4), 74-92. [https://doi.org/10.52326/jes.utm.2021.28\(4\).07](https://doi.org/10.52326/jes.utm.2021.28(4).07)

- Alexei, A., & Alexei, A. (2021). Cyber Security Threat Analysis In Higher Education Institutions As A Result Of Distance Learning. *International Journal of Scientific & Technology Research*, 10, 128-133. ISSN 2277-8616. https://ibn.idsi.md/vizualizare_articol/163773
- Alferidah, D. K., & Jhanjhi, N. Z. (2020, October). Cybersecurity impact over bigdata and iot growth. In *2020 International Conference on Computational Intelligence (ICCI)* (pp. 103-108). IEEE. <https://ieeexplore.ieee.org/abstract/document/9247722>
- Almaiah, M. A., Al-Khasawneh, A., & Althunibat, A. (2020). Exploring the critical challenges and factors influencing the E-learning system usage during COVID-19 pandemic. *Education and Information Technologies*, 25, 5261-5280. <https://doi.org/10.1007/s10639-020-10219-y>
- Alshammari, S. H. (2020). The Influence of Technical Support, Perceived Self-Efficacy, and Instructional Design on Students' Use of Learning Management Systems. *Turkish Online Journal of Distance Education*, 21(3), 112-141. <https://doi.org/10.17718/tojde.762034>
- Alwi, N. H. M., & Fan, I. S. (2010). E-learning and information security management. *International Journal of Digital Society (IJDS)*, 1(2), 148-156. <https://infonomics-society.org/wp-content/uploads/ijds/published-papers/volume-1-2010/E-Learning-and-Information-Security-Management.pdf>
- Antwi-Boampong, A. (2021). An Investigation into Barriers Impacting Against Faculty Blended Learning Adoption. *Turkish Online Journal of Distance Education*, 22(3), 281-292. <https://doi.org/10.17718/tojde.961849>
- Arko-Achemfuor, A. (2017). Student support gaps in an open distance learning context. *Issues in Educational Research*, 27(4), 658-676. <https://search.informit.org/doi/epdf/10.3316/informit.218315282267792>
- Bandara, I., Ioras, F. & Maher, K. (2014). Cyber Security Concerns in E-Learning Education. In: *Proceedings of ICERI2014 Conference* (728-734), IATED. <https://library.iated.org/view/BANDARA2014CYB>
- Bone, J. (2016). Cognitive Risk Framework for Cybersecurity: Bounded Rationality: Executive Summary: Part I. *EDPACS*, 54(5), 1-11. <https://doi.org/10.1080/07366981.2016.1247564>
- Brindley, J. E. (1987). *Attrition and completion in distance education: The student's perspective* (Doctoral dissertation, University of British Columbia). <https://open.library.ubc.ca/soa/cIRcle/collections/ubctheses/831/items/1.0054214>
- Chowdhury, N. H., Adam, M. T., & Teubner, T. (2020). Time pressure in human cybersecurity behavior: Theoretical framework and countermeasures. *Computers & Security*, 97, 101931. <https://doi.org/10.1016/j.cose.2020.101963>
- Creswell, J. W. (2013). *Research design: qualitative, quantitative, and mixed methods approaches* (4th Edition). London: Sage Publications.
- Çiftçi, A., & Karakuş, Y. (2019). Dijitalleşen Zamanın İzdüşümünde: Kimliğin, Bedenin ve İletişimin Dönüşümü. *AJIT-e: Bilişim Teknolojileri Online Dergisi*, 10(37), 7-30. <https://doi.org/10.5824/1309-1581.2019.2.001.x>
- Dhillon, M. (2020). Challenges and Issues of E-Learning. In *Emerging Trends in Big Data IoT, and Cybersecurity* (182-184).
- Durak, G. (2017). Uzaktan eğitimde destek hizmetlerine genel bakış: sorunlar ve eğilimler. *Açıköğretim Uygulamaları ve Araştırmaları Dergisi*, 3(4), 160-173. <https://dergipark.org.tr/en/pub/auad/issue/34247/378493>

- El Turk, S. & Cherney, I. (2016). Perceived online education barriers of administrators and faculty at a U.S. university in Lebanon. *Creighton Journal of Interdisciplinary Leadership*, 2(1), 5-31. <https://dx.doi.org/10.17062/CJIL.v2i1.30>
- Fırat, M. (2016). 21. Yüzyılda Uzaktan Öğretimde Paradigma Değişimi. *Yükseköğretim ve Bilim Dergisi*, 6(2), 142-150. <https://doi.org/10.5961/jhes.2016.151>
- Fırat, M. (2020). Öğrenci destek servislerinde doğal dil işleme: GPT-3 örneği. In *International Conference of Strategic Research in Social Science and Education* (pp. 532-536). 109 https://www.researchgate.net/profile/Mehmet-Firat-4/publication/347929179_Oğrenci_Destek_Servislerinde_Dogal_Dil_Isleme_GPT-3_Ornegi_Natural_Language_Processing_in_Student_Support_Services_Case_of_GPT-3/links/5fe7af9f45851553a0f5b455/Oğrenci-Destek-Servislerinde-Dogal-Dil-Isleme-GPT-3-Oernegi-Natural-Language-Processing-in-Student-Support-Services-Case-of-GPT-3.pdf
- Fırat, M. (2021). *Uygulamadan Kurama Açık ve Uzaktan Öğrenme* (2. Baskı). Nobel Yayınları.
- Fischer, E. A. (2016). *Cybersecurity issues and challenges: In brief*. <https://a51.nl/sites/default/files/pdf/R43831.pdf>
- Fraenkel, J. R., Wallen, N. E. & Hyun, H. H. (2012). *How to Design and Evaluate Research in Education* (8th Edition). New York: McGrae-Hill Companies.
- Genç Kumtepe, E., Toprak, E., Öztürk, A., Tuna Büyükköse, G., Kılınç, H., & Aydın Menderis, İ. (2019). Açık ve uzaktan öğrenmede destek hizmetleri: Yerelden küresele bir model önerisi. *Açıköğretim Uygulamaları ve Araştırmaları Dergisi*, 5(3), 41-80. <https://dergipark.org.tr/en/pub/auad/issue/50201/645975>
- Gutiérrez-Santiuste, E., Gámiz-Sánchez, V. M., & Gutiérrez-Pérez, J. (2015). MOOC & B-learning: Students' Barriers and Satisfaction in Formal and Non-formal Learning Environments. *Journal of Interactive Online Learning*, 13(3). <https://www.ncolr.org/jiol/issues/pdf/13.3.1.pdf>
- Gümüş, S. (2020). Açık ve Uzaktan Öğrenme Destek Hizmetlerinde Teknolojinin Kullanımı. M. Kesim & T. V. Yüzer (Eds.). *Açık ve Uzaktan Öğrenmenin Teknoloji Boyutu* (263-283). Ankara: Pegem Yayınları. 110
- IBM (2021). Why Human Error is #1 Cyber Security Threat to Business in 2021. Erişim Adresi: <https://thehackernews.com/2021/02/why-human-error-is-1-cyber-security.html#:~:text='Human%20error%20was%20a%20major,in%2095%25%20of%20all%20breaches.&text=Mitigation%20of%20human%20error%20must,cyber%20business%20security%20in%202021>. (Son erişim tarihi: 30.01.2022)
- Jang-Jaccard, J. & Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences*, 80(5), 973-993. <https://doi.org/10.1016/j.jcss.2014.02.005>
- Keast, D. A. (1997). Toward an effective model for implementing distance education programs. *American Journal of Distance Education*, 11(2), 39-55. <https://doi.org/10.1080/08923649709526960>
- Khanna, P. & Basak P. (2013). An OER architecture framework: Needs and design. *The International Review of Research in Open and Distributed Learning*, 14(1), 66-83. <https://doi.org/10.19173/irrodl.v14i1.1355>
- Lee, J. Y. (2003). Current status of learner support in distance education: emerging issues and directions for future research. *Asia Pacific Education Review*, 4(2), 181-188. <https://link.springer.com/article/10.1007/BF03025360>
- Li, J. H. (2018). Cyber security meets artificial intelligence: a survey. *Frontiers of Information Technology & Electronic Engineering*, 19(12), 1462-1474. <https://link.springer.com/article/10.1631/FITEE.1800573>

- Malyuk, A., & Miloslavskaya, N. (2016, July). Cybersecurity culture as an element of IT professional training. In *2016 Third International Conference on Digital Information Processing, Data Mining, and Wireless Communications (DIPDMWC)* (pp. 205-210). IEEE. <https://ieeexplore.ieee.org/abstract/document/7529390>
- Miles, M. B & Huberman, A. M. (1994). *Qualitative Data Analysis*. London: Sage Publication.
- Minh Hoang T. B., Dang-Pham, D., Hoang, A. P., Le Gia, B. & Nkhoma, M. (2020). Network Analytics for Improving Students' Cybersecurity Awareness in Online Learning Systems. In *2020 RIVF International Conference on Computing and Communication Technologies (RIVF)* (1-7). IEEE. <https://ieeexplore.ieee.org/abstract/document/9140781>
- Muilenburg, Y. L. & Berge, Z. (2005). Student barriers to online learning: a factor analytic study. *Distance Education*, 26(1), 29–48. <https://doi.org/10.1080/01587910500081269>
- Nespoli, P., Papamartzivanos, D., Mármol, F. G., & Kambourakis, G. (2018). Optimal countermeasures selection against cyber-attacks: A comprehensive survey on reaction frameworks. *IEEE Communications Surveys & Tutorials*, 20(2), 1361-1396. <https://ieeexplore.ieee.org/abstract/document/8169023>
- Okur, R. (2012). *Açık ve uzaktan öğrenmede öğretim elemanlarına yönelik çevrimiçi destek sistemi tasarımı* (Doctoral Dissertation, Anadolu University).
- Peters, O. (1993). Distance education in a postindustrial society. D. Keegan (Ed.). *Theoretical principles of distance education* (39-58). Routledge. <https://www.taylorfrancis.com/chapters/edit/10.4324/9780203983065-5/distance-education-postindustrial-society-otto-peters>
- Peters, O. (2002). *Distance education in transition: New trends and challenges* (5th Ed.). BIS Verlag. <https://oops.uni-oldenburg.de/550/2/petdis02.pdf>
- Peters, O. (2010). The theory of the „Most industrialized education“. *Distance education in transition: Developments and issues*, 11-32.
- Reegård, K., Blackett, C., & Katta, V. (2019). The concept of cybersecurity culture. In *29th European Safety and Reliability Conference* (pp. 4036-4043). doi: 10.3850/978-981-11-2724-3_0761-cd
- Rekkedal, T. (1981). *Introducing the Personal Tutor/Counsellor in the System of Distance Education*. Project Report 1: Experiment Description. <https://eric.ed.gov/?id=ED235774>
- Roddy, C., Amiet, D. L., Chung, J., Holt, C., Shaw, L., McKenzie, S., Garicaldis, F., Lodge, J. M. & Mundy, M. E. (2017). Applying best practice online learning, teaching, and support to intensive online environments: an integrative review. *Frontiers in Education* 2(59). <https://doi.org/10.3389/feduc.2017.00059>
- Sewart, D. (1980). Creating an information base for an individualized support system in distance education. *Distance Education*, 1(2), 171-187. <https://doi.org/10.1080/0158791800010204>
- Simon, H. A. (1955). A behavioral model of rational choice. *The quarterly journal of economics*, 69(1), 99-118. <https://doi.org/10.2307/1884852>
- Simon, H. A. (1972). Complexity and the representation of patterned sequences of symbols. *Psychological review*, 79(5), 369. <https://doi.org/10.1037/h0033118>
- Simon, H. A. (1976). From substantive to procedural rationality. In *25 years of economic theory* (65-86). Springer, Boston, MA. https://link.springer.com/chapter/10.1007/978-1-4613-4367-7_6
- Somayajulu, B. K., & Ramakrishna, T. (2008). Distance learners and support services: current trends and prospects. <https://oasis.col.org/items/dc6c32c1-75ea-4873-b82f-4f4240ee37e8>

- Thomas, G. (2021). *How to do your case study*. London: Sage. <https://www.torrossa.com/en/resources/an/5018110>
- Tuquero, J. M. (2011). A meta-ethnographic synthesis of support services in distance learning programs. *Journal of Information Technology Education*, 10, 157-179. <https://www.jite.informingscience.org/documents/Vol10/JITEv10IIPp157-179Tuquero974.pdf>
- Ulven, J. B., & Wangen, G. (2021). A systematic review of cybersecurity risks in higher education. *Future Internet*, 13(2), 39. <https://doi.org/10.3390/fi13020039>
- Udroiu, A. M. (2017). The cybersecurity of elearning platforms. In *Conference proceedings of eLearning and Software for Education «(eLSE)»* (Vol. 13, No. 01, pp. 374-379). Carol I National Defence University Publishing House. <https://www.cceol.com/search/article-detail?id=540463>
- Yıldırım, A. & Şimşek, H. (2013). *Sosyal Bilimlerde Nitel Araştırma Yöntemleri* (9. Baskı). Ankara: Seçkin.
- Yin, R. K. (2017). *Applications of case study research* (3th Ed.). London: Sage. <https://open.metu.edu.tr/handle/11511/70532>
- Yumurtacı, O. (2020). Öğrenen, Öğreten ve Teknoloji. M. Kesim & T. V. Yüzer (Eds.). *Açık ve Uzaktan Öğrenmenin Teknoloji Boyutu* (1-27). Ankara: Pegem Yayınları. 115
- Zawacki-Richter, O. (2019). The Industrialization Theory of Distance Education Revisited. I. Jund (Ed.). *Open and Distance Education Theory Revisited Implications for the Digital Era* (21-29). Springer: Singapore. https://link.springer.com/chapter/10.1007/978-981-13-7740-2_3
- Zhang, Z., Ning, H., Shi, F., Farha, F., Xu, Y., Xu, J., ... & Choo, K. K. R. (2021). Artificial intelligence in cyber security: research advances, challenges, and opportunities. *Artificial Intelligence Review*, 1-25. <https://doi.org/10.1007/s10462-021-09976-0>

Appendix-1: Interview Questions

1. How can technical support services be rationalized to ensure the safety of security experts and system stakeholders with bounded knowledge?
2. How can technical support service professionals with bounded capabilities in offensive prevention and defense activities be supported?
3. What kind of assessments can be provided as part of technical support services for security experts and system stakeholders with bounded assessment capabilities?
4. How can systems put at risk by the myriad uncertainties in cyberspace be analyzed in the context of technical support services?
5. How can security experts and system stakeholders with bounded decision-making capabilities be supported by technical support services?
6. How can technical support services structured around bounded information be mechanized to ensure cybersecurity?
7. How and through which mechanisms can the security activities provided within the bounded capability of technical support service experts be enriched?
8. How can the evaluation processes of technical support service experts with bounded evaluation skills be supported in the detection of cyber-attacks?
9. What techniques can be developed within the scope of technical support services to identify and assess the myriad uncertainties in cyberspace?
10. What mechanisms can be used to strengthen defense and detection decision systems controlled by individuals with bounded decision-making capacity and how?