The Communication Error Message: Managing Best Practice Ideas and the Cyber Threat. A Precursor to Communication Themes

Robert D. Boyd
Global Cyber Consultant
5661 NW 112TH Ave, Doral, FL 33178
Darshae_Kier@me.com

ABSTRACT

This publication explores the phenomenon of communication through the contextual lens of cyberspace operations. Using the cyberspace category and characteristics approach (C3A), this preliminary glance delves slightly deeper into how an organization can derive best-practice ideas to incorporate into everyday activities. This research showed that cyberspace practitioners who consented to foundational underpinnings of categorical and characteristic-based conditions of a cyber threat actor were in a better position to more efficiently and quickly assess an operational impact to an organization. Although it was important for the organization to determine its disposition commensurate to the threat actor, it was cyberspace practitioners who bought into the C3A that illuminated communication themes that were foundationally agreeable. The results of this research showed agreed-upon and streamlined thematic categories can result in innovative approaches to sharing dissimilar information across divergent areas.

KEYWORDS

best practices, cyberspace, threats, learning theory

1 INTRODUCTION

The notion of best practices must be revealed and incorporated throughout the organization between recognition of problem sets, communication of lessons learned, and implementation of best-practice ideas. Many best-practice ideas come as an effect of phenomenology. *Andragogy*, as defined by Knowles [1], is the "art and science of helping adults learn" (p. 54). Knowles, Holton, and Swanson [2] defined *andragogy* as "an intentional and professionally guided activity that aims at change in [the] adult person" (p. 60). Andragogy has come to be "synonymous with the education of adults" (Pratt [3], p. 160). The focus of this research addressed learning within the cyberspace practitioner community holistically. It removes the stigma that cyberspace operations equal cyber security. This is one of the fundamental reasons why articulating operational impact to an organization's leadership has become muddled and the conclusions on whether more tech-savvy people or communicators are needed are a topic of debate.

C3A is a step in the direction of removing the complexity in speaking across divergent communication fields and seeks to efficiently address cyberspace threat within an organization. C3A also exhibits a phased approach that can be leveraged by senior leaders, executives, and those with embryonic knowledge about the cyber security and cyberspace operations disciplines. This approach is important to the knowledge base as it more intuitively expresses and absorbs information illuminated by a cyberspace practitioner across categories, characteristics, and modi operandi within the field of learning. Knowles [4] concluded adults are self-directed learners, convey an affluence of experience to the academic setting, arrive to educational sceneries ready to learn, problem-centered in their learning, and principally stimulated by internal factors. C3A looks at analysis of how practitioners begin to describe indication and warning from an inherent independent understanding of what threat looks like through respective lenses. Upon such conclusions, the practitioners in this study recommended approaches to responding to a type of threat through learning how each other think comprehensively and independently about a given problem and then introduce that to cyberspace professional practitioners in other disciplines. Ultimately, the research addressed the complexity resident within the cyberspace practitioner field due to divergence in how information is understood and communicated from a cyber threat category and cyber threat characteristic-based perspective. The research further highlights the incorporation of these layers facilitate cyberspace practitioners' ability to more explicitly communicate their process for analyzing, interpreting, and responding to threat actions internal to and external from the organization. Further, the research results highlight the importance communication information transmitted verbally and translated binary to English for the senior-most echelons of organizations.

The research focus leveraged C3A to take an introductory look at shaping criteria for aiding organizations and their cyberspace practitioners categorically and characteristically. First, it addressed cyberspace practitioners' understanding of the meaning in the response assigned to a cyber threat actor utilizing a predetermined category that classifies the actor. Secondly, the research addresses how cyber practitioners can communicate risk to an organization before, during, and after a cyber threat actor action. Ultimately, by consenting to both categorical and characteristic conditions, cyber practitioners find themselves in a better position to assess and communicate the level of threat more easily. Understanding categorical and characteristic-based phenomena surrounding cyber threat actors describes Knowles's [5] fifth assumption of andragogy, that adults exhibit a familiarization and incitement to learn when they perceive that the learning will help them satisfy tasks or deal with predicaments that they confront in their life situations (pp. 57–63). Delving into the phenomena that are categorical and characteristic-based pertaining to cyberspace operations is a foundational underpinning from a professional life perspective.

It is understood that thematic categories (themes and messages) pertaining to threat and the applicable level of response are outlined and interpreted differently by different organizations. This, in many respects is why the categorization of level of advancement of the cyber actor and characterization of level of influence of the cyber actor is sometimes a challenge to agree upon. In C3A, two ways an organization and cyberspace practitioners can create linkages to communication barriers are (a) having mutual agreement of the interpretation of the threat category among cyberspace practitioners and the organizational support, and (b) having mutual agreement of the interpretation of the threat characteristics among cyberspace practitioners and the organizational support. Brookfield [6] noted that "learning is far too complex an activity for anyone to say with any real confidence an exact approach is likely to produce the most productive results with a particular category of the learner" (p. 122). There is certainly merit in this offering as the cyber security and cyberspace operations field changes by the minute. Even so, it is important to develop, at minimum, a point of departure that enhances communication and learning processes within this community of professionals to serve as a benchmark by which to grow towards in the future.

A point worth highlighting is the aforementioned bare degrees of comparison in interpretation of a category of cyber threat to that of a characteristic of cyber threat. First, there is a correlation of the cyber threat category to actions taken in and through cyberspace as being (a) passive, (b) active, or (c) hostile. Second, there is a correlation of the understanding of cyber threat characteristics to the frames of the actor's ability. In this sense, there must be a consideration for the (a) capability, (b) capacity, (c) intent, and (d) motivation of the actor to respond or influence a company, organization. or operation. Thus, correlating the two themes and subsequent elements of cyber threat category and cyber threat characteristic enhances an ability to transmit the communication of one cyberspace practitioner's code into the transcribing and verbalizing of another cyberspace practitioner's analysis in a way that can be received and understood by the external cyber audience. Currently, the field of adult learning appears to be toiling with inconclusive, paradoxical, and limited or inadequate empirical examinations (Brookfield [6], p. 91; Rachal [7], p. 211) and a "paucity of empirical research" (Beder & Carrera [8], p. 75). This pertains starkly to communication of and formulating best-practice ideas within the adult learning community. That community is also made up of a subset of the cyberspace practitioner community, in which such communication gaps are rampant.

This initial look at C3A serves to identify how different functional cyber practitioners can communicate and understand each other's interpretations about a cyber threat actor if there is agreement of the category and characterization of the variables of threat.

2 INTERPRETING CYBER THREAT

Threat is characterized differently to all who use the term to discuss network vulnerability, cyber actor capability, and operational assessment in which risk and outcome are considered. When utilized in the context of cyberspace, *threat* can be referred to as

- Any identified effort directed toward access to, exfiltration of, manipulation of, or impairment to the integrity, confidentiality, security, or availability of data, an application, or a federal system, without lawful authority.

- Potential cyber events that may cause unwanted outcomes resulting in harm to a system or organization. Threats may originate externally or internally and may originate from individuals or organizations.

The proposed working definition of *threat* is an applied knowledge of tactics, techniques, and procedures in a systematic manner with the expressed intent of causing harm to a system, individual, or organization. This research illustrates it can prove beneficial to understand not only the interpretation of threat by organizational cyber security practitioners but also the criteria utilized to bin such threats and communicate them across differing areas of functional cyber expertise.

Although there is a significant amount of information regarding the general background of learning theory (andragogy and pedagogy) and the divergence in communication bases, there is an absence of knowledge on the exploration and implementation of best-practice ideas (Knowles et al. [2]) that stems from a growth in communication. When considering the idea of binning cyber threats, a multitude of best-practice ideas can be considered. For instance, one approach is to categorize threat levels after first defining the category of threat.

Throughout this research, *cyber threat* is reviewed from an external actor perspective. The cyber actor's ability to impede or infringe upon an organization's networks continues to evolve; so must the communication of threat response based upon characteristics of the threat category, another possible best-practice idea once agreed upon and understood. Of note, the usage of cyber threat actor tools comparable to their frequency over time assists in classifying the categorical bracketing of passive, active, and hostile. As is discussed later in this research, intent and motivation are two of the four variables considered in the bracketing.

The capability and capacity of the cyber actor or influence from a more advanced actor such as a nation must also be considered and factored to truly comprehend and interpret the threat of the cyber actor. Language commonality must be promulgated in a way that it is transferrable to those seeking to understand and learn. Rogers (as cited in Bach, Haynes, & Smith [9]) articulated,

> I want to talk about learning. But not the lifeless, sterile, futile, quickly forgotten stuff that is crammed in to the mind of the poor helpless individual tied into his seat by ironclad bonds of conformity! I am talking about LEARNING—the insatiable curiosity that drives the adolescent boy to absorb everything he can see or hear or read about gasoline engines in order to improve the efficiency and speed of his "cruiser." (pp. 18-19)

As commercial, off-the-shelf tools become more accessible, the more nascent cyber threat actors or script kiddies will make it challenging to truly comprehend the reach of the cyber threat actor. Thus, common and foundational ways to communicate the categorization and characterization of the true threat posed by a cyber actor must be adopted. For this study, the terms *passive, active,* and *hostile* are utilized to describe threat categories and classify threat actor goals and organizational decisions that must be made based upon the level of the cyber actor threat. The categorical bracketing of threats is illustrated in greater detail later in this research as described by different functional cyberspace security and operations professionals.

Coming to agreement on such terminology and the underlying criteria used to define it can make providing information on indication and warning of cyber threats more understandable and less binary. What is interesting to note, however, is the diversity in the passive, active, and hostile threat categories and their meaning. This research first correlated the comprehension of the cyber threat category by events conducted in cyberspace from a network analyst perspective as being (a) passive, (b) active, or (c) hostile as indicated in Figure 1. Figure 1 explores of these thematic categories, illuminating terminology diversity and recommending communication inroads bridging technician and audience.

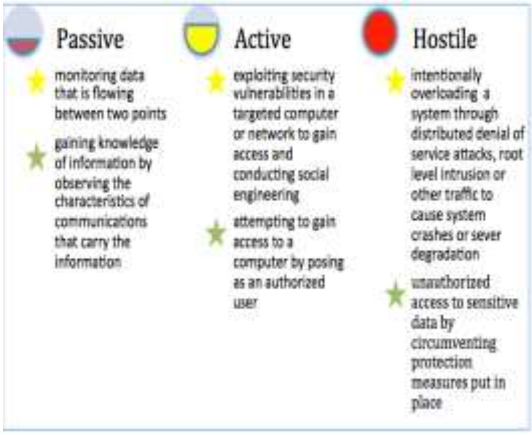
Passive
monitoring data that is flowing between two points
gaining knowledge of information by observing the characteristics of communications that carry the information
Active
exploiting security vulnerablities in a targeted computer or network to gain access and conducting social engineering
attempting to gain access to a computer by posing as an authorized user
Hostile
intentionally overloading a system through distributed denial of service attacks, root level intrusion or other traffic to cause system crashes or sever degradation
unauthorized access to sensitive data by circumventing protection measures put in place

Figure 1. Cyber network security cognitive thinking habits by cyber threat category.

Later, the research seeks to associate perceptions of cyber threat characteristics by the information intelligence analysts by reviewing a cyber actor’s ability, as seen in Figure 2. As is noted, network security analysts are generally concerned with manifestations that can be authenticated as passive, active, and hostile. However, information intelligence analysts often consider countenances of the (a) capability, (b) capacity, (c) intent, and (d) motivation of the cyber threat actor and the agreement of where the actor falls within the spectrum of the passive, active, and hostile categories.

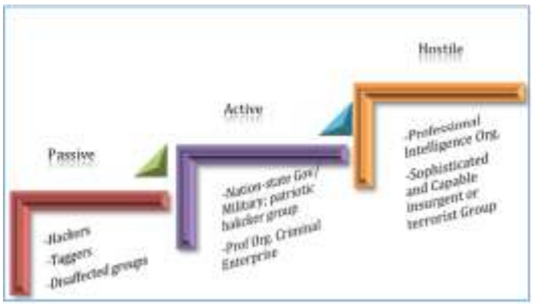
Passive
-Hackers
-Taggers
-Disaffected groups
Active
-Nation-state Gov/ Military; patriotic hakcker group
-Prof Org. Criminal Enterprise
Hostile
-Professional Intelligence Org.
-Sophisticated and Capable insurgent or terrorist Group

Figure 2. Information intelligence analyst cognitive thinking habits and characteristics by cyber threat category.

3 NETWORK SECURITY ANALYST

Network security analysts hold one of the most important roles in an organization in the thwarting of cyber threat actor advances into the network. To most, the language of firewall configurations, patching, STIGging, pen testing, and so on is unfamiliar to those not immersed within the community. From a job, task, and work role perspective, network analyst language is as foreign as heart surgery to a political science major.

Consider the term *firewall*. Network analysts set the boundaries of firewalls to do two things: (a) keep users from letting *bad stuff* into the network by blocking dirty words or sites with spam or malicious code and (b) keep cyber threat actors from attaining access. However, the ways in which a network analyst communicates cyber network security events and the way in which an information intelligence analyst or operations officer may receive the information are where the artistry must be discovered and translated. Not surprisingly, as many theorists have thus been less concerned with overt behavior than changes in the ways in which humans comprehend, perceive, or conceive the world around them (Ramsden [10], p. 4; Smith [11]). The divergence in communication sets by cyberspace practitioners must, too, be holistically viewed and not through linear lenses, in which message transmitted equals message received.

In its simplest form, a firewall is communicated as something that can sniff (search through) a packet of data for a precise match to the test listed in a filter. Many organizations have something known as a *hardware firewall*, which serves as a gateway (e.g., a Linksys cable/digital subscriber line router powering a home network). What does any of this mean in English? A firewall fundamentally blocks any annotation of a word or phrase variation that is an exact match to what is being referred.

Without neglecting the contextual description of network analyst language, hopefully one begins to see the gap in communication amid a tenable functional area and the transfer needed to make information useful to external audiences. Cyber network security analysts leverage these archetypes and apply them to their day-to-day practice to understand how the threat actor might impede upon networks.

The challenge is minimal when communicating this language to a group of peers. However, when speaking to executives, senior management, or even those that do not routinely operate at a tactical *into the weeds* level, understanding communication themes becomes increasingly important. In review of Figure 1, cyber network security analysts may be correct in their internal description of a cyber threat actor. Even so, there must be a way to interpret language into comprehendible information for those who need it to make decisions.

Although the nuances and technical intricacies of what could potentially be an update briefing on a network system or network intrusion are important, it does not translate into English for the external audience not versed in such terminology. The connection points to assist are seen in Figure 1, in which the cyber category (passive, active, and hostile) has been paired with summations characteristically used by a network threat analyst to describe cyber security events. The first star in each category in Figure 1 denotes terminology often used by these practitioners; the second star in each category denotes how such information can be interpreted and consumed.

The overlay of all three areas highlights agreements that must be made for C3A to be useful. First, there must be an agreement of governing cyber threat categories. Second, there must be recognition that cyberspace practitioners' terminology is not easily transferable to an external audience. Third, there must be an adherence to ensuring information can always be received contextually or verbally in a way that non–cyberspace practitioners can understand it.

As previously mentioned, the way information is communicated to external audiences measures the usability of the information. Thus, there must be an agreement with the information being communicated by divergent groups at a foundational level of learning by the cyber professionals who are collecting, fusing, and disseminating the information. Learning can be considered "a process by which behavior changes as a result of experience" (Maples & Webster as cited in Merriam & Caffarella [12], p. 124). Figure 1 considers language spoken by a network security analyst of a description of cyber threat activity and translates that into information for an external audience. Network security analysts persistently apply the ideological premise of passive, active, and hostile to a categorically based perspective. However, rarely is the communication of these network security analysts translated into a form that is comprehended by an external audience.

4 INFORMATION INTELLIGENCE ANALYST

Information intelligence analysts habitually communicate and research in a systematic and serial way to gather information. At times, this may introduce latency, thereby slowing the process to provide useful information to the organization. Although not inherently negative, this approach does not translate into an efficient way to communicate the weight of a threat of a cyberspace actor to an organization.

To unearth mutual interdependence and benefit to other cyber practitioners and exterior audiences, the thematic category of cyber threat characteristics bracketing, intelligibility of the cyber actor's intent, motivation, capacity, and capability should be leveraged. Cyber threat information can be seen as loaded with bias and, thus, is subject to perception and interpretation differently by external audiences. To reduce such bias, harmony on a foundational method to reinforce defining cyber characteristics of the

actor provides independent audiences with information supporting the assessment of the actor.
Figure 2 reviews potentialities for an information intelligence analyst to leverage the cognitive thinking habits characteristics collated with cyber categories and characteristics of the cyber actor levels. Note the contrast in descriptors utilized by these analysts over that of network security analysts in defining passive, active, and hostile categories. Network security analysts use the terminology to categorize the level of potential intrusion or event in the network or organization whereas information intelligence analysts often use the terminology as a mechanism to bracket the cyber threat actors, delineating the threat level to the organization and assessing possible ideological goals of the actor.

Thus, correlating characteristics of the cyber actor mark the question of where the characteristics of intent, motivation, capacity, and capability meet the categories of passive, active, and hostile.

As can be seen in Figure 2, the cyber categories of passive, active, and hostile have been coupled with summations characteristically used by an information intelligence analyst to illustrate what passive, active, and hostile represent when paired with a cyber actor. In order for Figure 2 to be seen as information that can be transferable, there must be a consideration for the attending audience. Understanding requires agreement of the cyber threat characteristics variables by the information intelligence analyst paired with cyber threat type to align the assessment to transferable information.

The aforementioned variables present a communication inroad between two disciplines, coupling the cyber category and cyber characteristics. They allow the information intelligence analyst to prepare for discussions with an executive or operations officer to achieve usefulness in communicated information. Both areas are of vital importance because operations officers' interests are in both areas of cyber category and cyber characteristics. They are both the planners and likely the briefers of the culminated information from these practitioners.

5 OPERATIONS OFFICER

Figure 3 represents the operations officer decision cycle by cyber threat category and characteristics of the analytic mindset. Operations officers are of the analytic mindset. These officers begin to associate cyber threat categories and characteristics to identify and communicate information that would be found useful to the operations officer and further describe how the operations officer conventionally reflects concerning cyber operations. Together, C3A capitalizes on the diversity of verbiage spoken and accommodates thematic categories, in which such information can be deciphered and transferred.

Figure 3 accents all functional areas must have some measure of agreement as to the inception for reporting of passive, active, and hostile events, irrespective of a utilitarian area. Note that each threshold necessitates some level of decision.

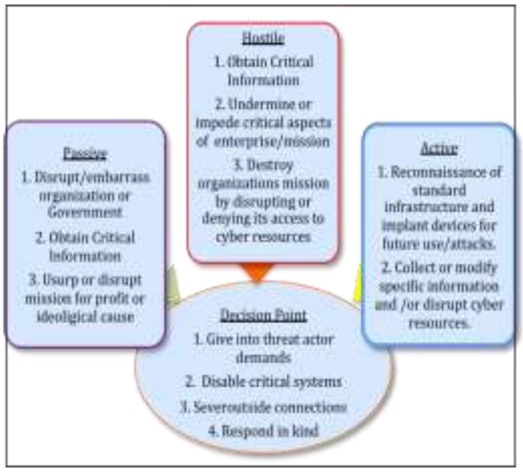
Hostile
1. Obtain Critical Information
2. Undermine or impede critical aspects of enterprise/mission
3. Destroy organizations mission by disrupting or denying its access to cyber resources
Passive
1. Disrupt/embarrass organization or Government
2. Obtain Critical Information
3. Usurp or disrupt mission for profit or ideoligical cause
Active
1. Reconnaissance of standard infrastructure and implant devices for future use/attacks.
2. Collect or modify specific information and /or disrupt cyber resources.
Decision Point
1. Give into threat actor demands
2. Disable critical systems
3. Severoutside connections
4. Respond in kind

Figure 3. Operations officer characteristics of the analytic mindset and decision cycle by cyber threat category .

From a categorical identification perspective, Figure 3 contains both thematic categories. There is a description of what could potentially be seen as cyber threat characteristics in relation to the cyber threat actor type in Figure 2. For example, a hacker, as described in the passive category in Figure 2, would seek to achieve the objective as specified in the passive category listed in Figure 3. This gives information intelligence analysts a glimpse into the mind of operations officers and how they think about the threat actor being addressed by the provided assessment.

Figure 3 also illustrates how each decision point accentuates a level of impact. Cyber security functional practitioners must be able to understand the risk in relation to the cyber category and characteristic of the threat to inform decision makers. Although not as simple as following a left-to-right, up-then-down model, C3A illustrates there can be a level of ease that can be correlated to communication themes when cyber practitioners understand and agree upon an efficient approach. For example, the network security analyst may suggest that severing a connection to a server will diminish the cyber actor's access to the intranet of the organization. However, the operational impact connected with such action means the company may also lose access to their internal systems. A secondary effect would be a possible loss of access to organizational records and files of clients and employees. The information intelligence officer may contribute details of a cyber threat actor based upon information known from the type of actor. Ultimately, if there is not a foundational way of understanding what is important to each functional practitioner, there will be vacuums of information, thereby leading to latency in understanding what is actually needed.

6 CONCLUSION

Knowles [1] acknowledged that adult learners must be able to understand the context and reason behind learning. Such a statement holds true when efficient and accurate operations decision making must be done to inform a wider, less technically savvy community.

C3A aims to present that the phenomenon of communication is experienced by functional practitioners differently and serves as an amalgamation of thematic narrative through graphical representation and better practice recommendation. If best-practice ideas are derived from agreed-upon thematic categories of said phenomena, the future proof of identity and communication of divergent data sets may be found more agreeable across different knowledge bases. Within foundation, the second assumption of Knowles's [1] six principles of learning, Knowles suggested that experiences of the learner, including errors and successes, are the foundation for learning. Cyberspace professionals must identify the foundational errors that reside within communication divergence and attack those areas instead of the complex, stratospheric problems. Technology is ever changing and the conveyance of the diverseness of introspection is innately a cognitive and active (experience-based) manifestation. Thus, discernment by the members of an organization and successful conveyance of these knowledge bases to internal organizational leaders and external partners are inescapably entwined with the benchmarking of knowledge bases through dialogic conversation.

As illustrated in Figure 1, the rather semitechnological to technical intricacy to explain computer-based vulnerability within organizations is complex. Figure 2 illustrates that albeit the same language is being expounded verbally, interpretation and resonation may be disparate, without interchangeable agreement of what is important. Figure 3 demonstrates that risk is affiliated with each level of category and characterization of the cyber actor, irrespective of agreement. Self-concept, another assumption of Knowles's [1], suggests that in order for learning to take place, adults must recognize that they need to be involved in planning and evaluating their instructional activities.

The cyber security community is at a time in which agreements of thematic categories to share information with leaders must be considered and applied in order to deliver near-real-time recommendation of possible events.

C3A illuminates the differences that are prevalent in the way in which operating areas communicate their version of English within and outside of the community. For a moment, consider how that would change if better practice ideas that linked divergent thoughts across shared themes were in place. Such thematic reasoning could then be applied to industry, the private sector, academia, and government.

C3A provides a method to identify the differences in communication among cyber practitioners and why they exist. Communication gaps, in this case, are attributed to education, personality types, experience, and comprehension of other working areas by measurement and definition of vulnerability and threat. Others are attributed to austere communication gaps across the three areas of the environment. This initial look at C3A reviewed research of functional cyber professionals' understanding of how cyber threat category is perceived and linked to their consciousness of the characteristics of cyber threat. Further, C3A highlights that an agreement between cyber category and characteristics will allow for possible discovery of better practice ideas within organizations. The overlay of all areas highlights agreements that must be made for C3A to be useful. From a best-practice idea perspective, there must be an agreement of governing cyber threat categories. Second, there must be recognition that practitioners' terminology is not easily transferable to an external audience and the C3A foundational premise or one similar should be leveraged. Third, it must be ensured that information can always be received contextually or verbally in a way that non–cyber practitioners can understand it.

There must be a sensible effort to agree to weights defining the categories of passive, active, and hostile to communicate effectively. There must also be a conscious effort to make sense of the characteristics of intent, motivation, capacity, and capability and apply these criteria to the cyber actor. In this community, a theme without a category is like a category absent from a characteristic. Thus, if there is a thematic category (i.e., variable of mutual agreement), there is a characteristic representative of a theme that is useful to most any audience.

REFERENCES

1. Knowles, M. S.: The Adult Learner: A Neglected Species (4th ed.). Gulf, Houston, TX (1990).
2. Knowles, M. S., Holton, E. F., III, Swanson, R. A.: The Adult Learner: The Definitive Classic (6th ed.). Elsevier, Burlington, MA (2005).
3. Pratt, D. D.: Andragogy as a Relational Construct. Adult Education Quarterly 38, 160–172 (1988, Spring).
4. Knowles, M. S.: The Modern Practice of Adult Education: Andragogy Versus Pedagogy. Prentice Hall/Cambridge, Englewood Cliffs, NJ (1970).
5. Knowles, M. S.: Andragogy in Action: Applying Modern Principles of Adult Learning. Jossey-Bass, San Francisco (1984).
6. Brookfield, S. D.: Understanding and Facilitating Adult Learning. A Comprehensive Analysis of Principles and Effective Practices. Open University Press, Buckingham, England (1986).
7. Rachal, J. R.: Andragogy's Detectives: A Critique of the Present and a Proposal for the Future. Adult Education Quarterly 52, 210–227 (2002, May).
8. Beder, H., Carrera, N.: The Effects of Andragogical Teacher Training on Adult Students' Attendance and Evaluation of Their Teachers. Adult Education Quarterly 38, 75–87 (1988, Winter).
9. Bach, S., Haynes, P. Smith, J. L.: Online Learning and Teaching in Higher Education. McGraw-Hill, New York, 18-19 (2007).
10. Ramsden, P.: Learning to Teach in Higher Education. Routledge, London (1992).
11. Smith, M. K.: Learning Theory: Models, Product and Process, http://infed.org/mobi/learning-theory-models-product-and-process/ (2003).
12. Merriam, S. B., Caffarella, R. S.: Learning in Adulthood: A Comprehensive Guide (2nd ed.). Jossey-Bass, San Francisco (1998).