Behavior and Social Issues
https://doi.org/10.1007/s42822-024-00174-5

ORIGINAL PAPER

Systematic Analysis of Individuals' Perspectives on Cybersecurity Using Q Methodology: Implications for Research and Application in Behavior Analysis

Rita Olla[1] · Ramona A. Houmanfar[1] · Shamik Sengupta[2] · Emily M. Hand[2] · Sushil J. Louis[2]

Accepted: 5 April 2024

Abstract

Emerging sociocultural challenges such as malicious cybersecurity attacks and the cyber-unsafe utilization of the internet across industries highlight ways analysis of consumer perspectives pertaining to products of behavioral systems (e.g., government, universities, and business) may inform interventions relating to secure cyber-behaviors. In this study, we conducted a systematic analysis of viewpoints for two groups of college students (computer science and psychology majors) on cybersecurity using a Q methodology approach. The analysis revealed three shared viewpoints. The first one highlighted the importance of facing the security of internet utilization at the level of the entire society, thus suggesting the supply of appropriate cyber training for any type of internet users. The second viewpoint communicated a shared concern for the inability of businesses and the U.S. government to protect the privacy of their users effectively. The third viewpoint, which was only communicated by the psychology major students, emphasized the risks of cyberspace but also expressed difficulties in meeting the requirements associated with users' safe access to the internet. These types of findings offer guidance for community leaders in making decisions about educational interventions, while accounting for the perspectives of potential recipients of educational services as part of addressing social validity concerns (see Baer et al. *Journal of Applied Behavior Analysis, 1*(1), 91–97, 1968).

Keywords Assessment tool · Community interventions · Cybersecurity education · Q methodology · Social validity

The acquisition of behavioral repertoires, essential for functioning effectively in society, necessitates the creation and application of appropriate learning contingencies (Skinner, 1938, 1953, 1965, 1968). Educational institutions play a crucial role in this process by implementing training programs that inform the community of

Extended author information available on the last page of the article

Published online: 11 June 2024

students who will contribute to the growing work force across industries (Krapfl & Gasparotto, 1982; Malott, 2003, 2022). With the expanding role of social networks in our global landscape (e.g., Facebook, X -*ex Twitter*, Instagram, TikTok) opportunities for intra- and interindividual transmission of adaptive and maladaptive behaviors inside and outside of organizations are limitless.

The challenge is to organize massive numbers of people to participate in cultural practices (Glenn, 2004) that are adaptable to the constantly evolving digital technologies in ways that are conducive to the survival and advancement of cultural groups. Influencing behavioral patterns of hundreds, thousands, millions, or even billions of people will require changes in many environmental sources of influence on resource consumption such as institutions, social groups, private and public organizations.

Houmanfar et al. (2009) and Houmanfar and Szarko (2022) discussed the functional account of organizational change via focus on leadership practices in the context of behavioral systems analysis (BSA; Krapfl & Gasparotto, 1982; Malott, 2003, 2022; Malott & Glenn, 2006; Mawhinney, 1992). This approach orients the investigative focus "on the of behavior that occurs [within] complex and organized social environments" (Krapfl & Gasparotto, 1982, p. 22), allowing for the systematic identification of critical participatory factors in dynamic behavioral systems (Malott, 2003, 2022), instead of looking only at the behavioral contingencies as they occur at the level of the single individuals. According to Malott's (2003, 2022) Behavioral Systems Engineering (BSE) Model, which is based on general system theory and coherently builds on BSA, organizations are behavioral systems that are formed by individuals' interaction toward a common objective (defined as aggregate product). This interaction toward a common objective occurs within the context of the organization's interaction with a broader sociocultural and economic environment (Brethower, 1982, 1999, 2000; Glenn & Malott, 2004; Krapfl & Gasparotto, 1982; Malott, 2003, 2022; Malott & Glenn, 2006; Rummler, 2001; Rummler & Brache, 1995).

Approaching systemic change by identifying key environmental factors that influence patterns of behaviors, particularly behaviors of those who design and implement organizational contingencies (i.e., organizational leaders) in target organized groups (i.e., organizations), plus their aggregate products affecting consumer practices (Alavosius et al., 2017; Houmanfar et al., 2015) may lead to practical and effective solutions to social problems such as cybersecurity and emerging challenges associated with the internet utilization. In this context, the perspectives of consumers and their feedback in terms of value adding nature of aggregate products are critical to the success of leadership decision making and associated changes in organizational practices (Houmanfar et al., 2009, 2015). The consumer side of behavioral systems analysis has been largely ignored within behavior analysis. It is fortunate that recent literature in organizational applications of behavior analysis has laid substantial groundwork for an advanced analysis of consumer behavior (e.g., Foxall, 1999, 2001, 2010, 2015; Hantula et al., 2001).

In addition, educational considerations are pertinent across various disciplines and social issues, which community leaders must address. For example, there is a growing concern regarding cybersecurity across different industries. It highlights the need to educate future cyberexperts in a way that encompasses these broader social challenges, as well as regular internet users who necessarily contribute to the reliable functioning of the cyberprotocols. Therefore, in this article, first, we briefly report the current challenges in cybersecurity. We then introduce the Q methodology (Q; Brown, 1980, 1986) as a tool to investigate college students' perspectives on this issue. According to the BSE framework (Malott, 2003, 2022), students are considered the recipients (i.e. consumers) of the services provided by the educational system. They constitute one of the selecting environmental factors (i.e., consumers) that interact with what is offered by the educational subsystem (Malott, 2003, 2022). Based on the *consumption* of the available educational aggregate product, students should be able to correctly engage within the cybersecurity domain both as potential future developers of cyberprocedures and as everyday internet users.

Finally, using the Q study findings, and referring to the principles of behavior analysis applied within the BSE framework (Malott, 2003, 2022), we propose educational content to prepare not only future cyber-experts but also equip regular internet users with essential cybersafety knowledge. The latter in particular can either contribute to solving cybersecurity challenges if appropriately educated, or exacerbate them if not properly included in intervention strategies.

Societal Consequences from Cybersecurity's Challenges

The concept of cyberspace has become an integral part of modern human experience as a cultural practice that is present in a range of contexts from simple recordkeeping to complex space missions. Hence, security from modern day attacks of hackers, terrorists, or skilled corporate raiders has become a critical issue for all cyberconsumers. Cybercrimes, in fact, can cripple global economies and are expected to inflict damages up to $10.5 trillion by 2025 (Freeze, 2022). Important services such as health-care systems, enterprise networks, and governmental organizations are becoming targets for these attacks (Robertson & Chapa, 2022). For instance, a cyberattack against the United Nations in April 2021 gave cybercriminals access to sensitive networks through the usage of stolen user credentials that were purchased on the dark web (Turton & Mehrotra, 2021). However, evidence suggests that secure cyberspace cannot be realized by technology alone as it extends beyond the narrow technical concepts of computer security and cryptography. Although the importance of computer security and cryptography cannot be minimized, a secure cyberspace encompasses both technological and human aspects.

Despite the recognition of the above needs, a majority of cybersecurity professionals are equipped primarily with a technical background and are focused on securing systems based on purely technical metrics without accounting for crucial nontechnical factors, those relating to social and behavioral factors. From a technical professional's perspective, many system designs reach a point where human factors and/or risk management issues become involved; it is here that the inability to account for such issues often leads to vulnerabilities within the systems. It is therefore crucial that the next generation of cybersecurity workforce is appropriately educated and equipped with an all-encompassing understanding of technical, political, social, and human factors within a cyberspace context, thereby enabling them to understand the critical objectives of cybersecurity's mission. Furthermore, it is important to design appropriate educational programs for ordinary internet users, whether as consumers of online products or service providers, while accounting for their limited expertise in cybersecurity and their historical interactions as nonexpert users.

Purpose of Study

Building on these premises about the extensive risks associated with the increasing cybercriminal activity and the recognized necessity to educate the future generations of developers and users of cyberprotocols, this study aimed to identify perspectives about cybersecurity-related behaviors communicated by senior college students majoring in computer science and in psychology. This combination of participants with different areas of training was designed to capture the viewpoints of groups of internet users with and without formal computer science training. The latter make up a large subset of internet service consumers, employees, managers, and professionals who heavily operate online, the majority of whom are often the first target of cybercriminals' attacks.

Hence, the experimental questions consisted of the following: (1) What are the ways college students describe their opinions about safe access digital services? (2) In what ways does education in computer science influence the students' viewpoints? (3) How do the college student viewpoints align with an expert who teaches and conducts research in cybersecurity?

It should be noted that, as highlighted by Ramlo and Nicholas (2020, 2021), investigative analysis about people's opinions on cybersecurity usually can take the form of either broadly distributed surveys (such those promoted by the Pew Research Center; Olmstead & Smith, 2017) or the form of direct interviews involving small group of participants (Aljuaid & Liu, 2023; Cusak, 2023; Thompson et al., 2018). However, with respect to these two research methodologies "somewhere in between a large quantitative study [like the Pew research] and a small qualitative study, [there is the space for] a deep investigation into revealing and describing the divergent views of cybersecurity using Q methodology" (Ramlo & Nicholas, 2020, p. 1).

Q Methodology

William Stephenson (1935a, b, 1936, 1953a, 1978, 1980, 1993), who first introduced the methodology, suggested applying factor analysis techniques, in its inverted form,[1] to identify similarity of individuals' patterns of viewpoints or perspectives instead of averaged results of the tests or surveys administrated to groups. Stephenson's approach was labeled as Q methodology to distinguish it from other approaches. In 1936, he wrote

> I have agreed with a suggestion made by Prof. G. H. Thomson [1935] that r [technique, or R as it is currently referred to, Brown et al., 2007] will stand for correlations between tests, etc. as variables, while Q will stand for correlation between persons as variables. The present-day factor technique may therefore be designated r-technique, and the **inverted form**, Q-technique. (p. 353, boldface added)

This is an interesting distinction because it reveals the measures are samples of group averages or individual metrics. Stephenson (1953a) used the Q for his study of *subjectivity*, which he identified as a legitimate subject matter susceptible to scientific investigation (Burt & Stephenson, 1939). In the Q dictionary, subjectivity "is regarded as a person's communication of a point of view on any matter of personal or social importance" (McKeown & Thomas, 2013, p. ix). In more detail, it refers to "things that we say—silently to ourselves . . . or publicly to others as in conversation—from our own vantage point, and excluding that which is objective" (Brown, 2019, p. 565). Brown (1980) makes explicit Stephenson's naturalistic approach when discussing this seemingly cognitive term:

> Fundamentally, a person's subjectivity is merely his own point of view. It is neither a trait nor a variable, nor is it fruitful to regard it as a tributary emanating from some subterranean 'stream of consciousness.' It is simply a *private behavior* [emphasis added] that we engage in during the normal course of the

[1] Factor Analysis (FA) (Adcock, 1954; Kline, 1994) is a statistical method that was developed in 1904 by Charles Spearman (Lovie & Lovie, 1996) with whom William Stephenson graduated and worked. As statistical tool, FA is used to analyze variability in sets of variables (coming from multiple sources such as, for example, our internet navigation choices), in search of correlations among the variables themselves so that their numerosity can be potentially reduced to a smaller number of unobserved ones called factors. FA is currently applied in (a) machine learning to allow the estimated models to focus on a smaller number of variables, improving the model interpretability and often its predictive performance, (b) risk management and portfolio analysis to identify underlying factors that affect asset prices or returns, and (c) marketing to capture consumers' preferences, and possibly identify underlying "factors" in consumer behavior, to cite just a few domains. This specific use of the FA is what Stephenson refers to as r (or R) technique, and it looks at the variability of variables coming from tests, or other measurement and data collection systems (Brown & Melamed, 1990). Within the Q methodology, however, Stephenson demonstrated that the same algorithm could be used to "factorize" people who have similar –correlated– opinions that Stephenson defined as subjectivities expressed via operant behavior, like the sorting activity performed by the participants when presented with the research stimuli, as described in this section. In this sense, for Stephenson "Q-technique opens an *entirely new field*" for psychological study (Burt & Stephenson, 1939, p. 280, italics added), namely the study of subjectivity expressed via operant behavior.

> day. To say that a particular kind of behavior is subjective, however, is not to preclude measurement, for it is the explicit objective of Q technique to allow a person to express "his subjectivity operantly, modeling it in some manner as a Q sort." (Stephenson, 1968, p. 501) (p. 46)

With respect to Q as assessment tool, Brown (1980) explains that when people are asked to express their viewpoints via the sorting of the presented stimuli (as later described in detail) , their behavior is "both *subjective* and *operant*. It is subjective because each persons' viewpoint, on political or any other matters, is simply that—his viewpoint. It is *operant* because it occurs naturally within a particular setting" (Skinner, 1953; p. 4, emphasis added; Brown, 2016; Delprato & Brown, 2002; Stephenson, 1970, 1977; Watts, 2011).

Stephenson clearly expressed his appreciation for B. F. Skinner's research and Kantor's naturalistic psychology in his investigation on how to measure individual subjectivity (Stephenson, 1953b, 1977, 1979). Other publications have highlighted Stephenson's alignment with Skinner's radical behaviorism, and Kantor's interbehaviorism: Brown (1994, 2002a, b, 2006), Delprato and Brown (2002), Delprato and Knapp (1994), Midgley (2005), and Midgley and Morris (2002).

It is important to note that Q provides an alternative approach to forced-choice surveys for the identification of what can emerge as *unexpected* groups of individuals who share *similar* opinions, by providing more nuanced information compared to simple averages (Brown, 1999). Moreover, traditional surveys, designed to capture the opinions of the interviewees, and analyzed via univariate or multivariate statistical techniques (e.g., ANOVA or MANOVA), embed response scales whose meaning is defined by the researcher themselves or by the theory that the survey is meant to test or verify. Furthermore, the format of measurement scales employed in the survey (e.g., ordinal or nominal) affect the way in which the data are statistically analyzed and subsequently explained (Brewer-Deluce et al., 2020; Brown, 1980, 1986, 1999; Rhoads, 2001; Rhoads & Sun, 1994).

Another important note regarding Q is its utility in the area of conflict management and development of cooperation among groups (Brown, 1980, 1986, 1993; Durning & Brown, 2006; Maxwell, & Brown, 1999; McKeown & Thomas, 2013; Stephenson, 1935a, b, 1936, 1953a). Durning and Brown (2006), and Brown et al. (2007) provide an extensive review of how a Q approach can provide support to the leaders often in need of "information and recommendations to assist them in distinguishing among choices and in finding compromise solutions for controversial issues" (Durning & Brown, 2006, p. 555). In this regard, Q studies can be designed not only to identify different viewpoints and understand what makes them different or similar (with respect to some aspects) to other perspectives, but also to provide the context, the competing problems, or help to figure out solutions for intractable (wicked) problems (van Eeten, 2001).

According to the Q technique, people's opinions are collected by presenting them with a set of stimuli, called *Q set*. The Q set represents a structured (Brown et al., 2019, Fisher, 1971) subset of stimuli sampled from the *universe* of the stimuli—called *concourse*. The concourse includes what is communicated and shared as opinions (not as objective facts, such as the capitol of the United States) in a community

Table 1 The sorting grid

	Most UNLIKE my view					Neutral					Most LIKE my view
score	-5	-4	-3	-2	-1	0	+1	+2	+3	+4	+5
Frequency	2	3	4	5	6	7	6	5	4	3	2

The table reports how the sorting was organized. It allowed scores from -5 to + 5 (an 11-point scale). The maximum numbers of statements allowed per score is reported in the row Frequency. For example, only two statements could be placed at the extreme poles, -5 and + 5, whereas seven statements could be assigned to the score 0.

about any given topic (in our study, the opinions on cybersecurity). The stimuli included in a Q study are often in the form of verbal statements, but other types of stimuli have been used such as fonts (Buehner, 2011), photos of different content, like food (Simpson, 1989), people of different gender and ethnicity (Kuipers et al., 2022), children's preferences in play settings (Hempel, 2021), wildfires (Duan et al., 2021), tourism locations (Fairweather & Swaffield, 2002), paintings (Somerstein, 2014), cartoons (Kinsey, 1993), movies (Robinson et al., 2014), news pictures (Stephenson, 1960), colors (Stephenson, 1936), and country music (Wacholtz, 1992a, b). In this study, we used written statements in English language. The participants recruited for the study compose the *P set.* In particular, the selection of the P set is structured to adhere to Fisher's (1971) experimental design, as a balanced group including different *types* of participants. Thompson (1886–1966) suggested, as a possible strategy, to identify participants in terms of their *opinion type*. Stephenson (1964) clarifies this aspect. Hence, we can have:

1. participants who have a *special* interest in the topic under investigation;
2. participants who are *experts* (Stephenson [1964] specifies that they are "persons of maturity, broad education and experience, who, given all the pertinent facts on the controversy, are asked to form a dispassionate judgment on the controversy" [p. 270]);
3. participants who are *existing authorities* ("those who take it upon themselves to speak for one side or the other of [the topic under discussion]" [Stephenson, 1964, p. 270]);
4. participants who have *class* interests with respect to the topic (e.g., typical demographic or social groups such as, residents versus immigrants, young versus elderly, gender A versus gender B, to provide a few examples); and
5. *uninformed* participants (that Stephenson suggests considering as a control group for the other interests: "people who know little about the matters under [discussion], and who care even less" [Stephenson, 1964, p. 270]).

Participants sort the statements on a provided sorting grid (see Table 1 for the grid used in this study) guided by the *condition of instructions*, the technical term used to indicate how the participants are instructed to address and evaluate the stimuli presented by the researcher. The sorting grid offers the participants the opportunity to express a dual and opposite evaluation of the statements—most positive and most negative—as well as a space, in the center of the grid, for less intense reactions to the items (Brown, 2019). The final display of the sorted statements on the grid comprises the Q sort, which represents the participant' *whole* opinion or subjectivity (Brown, 2019; Midgley & Delprato, 2017; Midgley & Morris, 2002; Ramlo, 2022; Stephenson, 1977). Participants' comments about the statements that they placed at the extreme poles are collected and guide the researcher's interpretation of the *group Q sorts* called factor arrays or composite factor that emerge from the statistical analysis. The analytical procedure includes a stepwise implementation of the following: (1) correlation of each Q sort to all other Q sorts; (2) factor analysis of the correlation matrix; and (3) factor extraction, and rotation. The final analytical step that makes Q technique unique comprises of the calculation of the *factor arrays.* This phase implies the calculation of the standardized scores for the statements within each extracted factor thus making "possible direct comparison with scores for the same statements" (Brown, 1980, p. 243) for all emerged factors, i.e., viewpoints. In this context, the factor arrays are to be considered the *theoretical* Q sort for each identified group of individuals. Factor array interpretation (Albright et al., 2020) starts by looking at which statements are placed at the extremes of the poles, which statements have a similar position on the other groups' arrays (these statements are called *consensus* statements), and which statements occupy a statistically significant different position ($p < 0.01$) on each factor arrays (these statements are called *distinguishing* statements).

A final important note about the Q approach is that with this methodology, it is possible to *define* groups of individuals that are not based on *a-priori* traditional social or demographic features or established by the researcher. Given that individuals belonging to different categories may share similar opinions, Q enables the discovery of *unexpected* opinion groups within a community (Brown, 1980). Therefore, these findings may support the development and implementation of better interventions because their content can be designed closer to people's opinions rather than the demographic features of the class to which the people have been assigned.

The following sections provide a detailed overview of the research methodology and associated procedures. We will follow with a summary of findings and discussion.

Method

P Set: The Participants

Forty-six individuals who participated in this study were college seniors enrolled in a public university in the southwest region of the United States. Twenty-two were computer science majors who were recruited while attending a class on cybersecurity; 23 were psychology majors. The latter were recruited through an online platform implemented by the university's department of psychology. The study was advertised using flyers and informing other psychology class instructors about the availability of the research so that the information could be shared with their students. The students' participation was, however, on a voluntary basis by signing up in the online platform. The expert/professor of the cybersecurity course at the target university participated in the study too. The students received compensation for their participation (which lasted an average of 30 min; no fixed time to complete the Q sorting activity was imposed) in the form of extra credit in their classes and the chance to win one of two $15 Amazon gift cards, one randomly assigned to each group of students. (Appendix 1 includes Tables 3, 4, and 5, containing participants' demographic information related to age, gender, and citizenship.) The P set composition followed Fisher's experimental design (Fisher, 1971, Brown, 1980, 1986; Brown et al., 2019). In this study, the inclusion of a single expert, who also served as the instructor for the cybersecurity class, aimed to ascertain whether the students enrolled in the class would share their opinions with that of their instructor.

Q Set: The Statements

Forty-seven statements (see Appendix 2) were used in the current study. These statements were adopted, verbatim, from Ramlo and Nicholas (2020, 2021). The authors provide detailed information about the sampling of the Q set from the concourse they developed in their 2020 paper.

Procedure

Data Collection

The online platform QSortouch (https://qsortouch.com/) was used to collect the opinions (Q sorts) of the participants. The IRB consent form was uploaded onto the platform and participants had to check a box to accept it before moving on to the next parts of the task. The 47 statements (see Appendix 2) were uploaded, alongside the *conditions of instructions*, according to which each statement in the sorting activity was addressed.

Participants were asked to provide their comments about the statements they placed at the extremes of the sorting grid and to fill out a short survey for demographic information. (Tables 3, 4 and 5 include information about participants' age, gender, and citizenship; see Appendix 1). The sorting activity occurred in two phases (Brown, 1980). First, the participants were asked to read the statements which were presented randomly one-by-one and assign them to one of three piles available: (1) statements for which the participant noted agreement (or alignment); (2) statements for which they noted disagreement; and (3) statements for which the participants had a neutral opinion or an opinion that could be different under different circumstances. There was no constraint on the number of statements the participants could assign to each pile.

The second phase allowed the participants to refine their opinion about the statements using the provided sorting grid (see Table 1 reporting the scores used and the number of statements that could be assigned to each score). In this phase, the participants were asked to sort the statements previously divided into the three piles, by assigning them a score ranging from -5 (Mostly UNLIKE my view) to +5 (Mostly LIKE my view) and placing them on the appropriate slots on the grid. The sorting grid had a quasi-normal distribution shape and the number of statements for each score was fixed (thus representing an example of forced distribution; Brown, 1980, 1986). For example, the score of -2 (or +2) could be assigned to no more or fewer than five statements. Participants could freely move all the items on the grid until they identified their preferred allocation before they submitted their Q sort. An important aspect of the Q sorting activity is that the participant scores each statement in relation to the others, rather than as independent items as arranged in traditional surveys. After the participants submitted their Q sort, they were asked to provide a comment as to why they placed certain statements on the poles of the grid (-5 and + 5). All participants, excluding the expert, left their comments.

It is important to highlight that the scoring range presented in the grid, which guides participants on where to place statements they most agree or disagree with, is not a Likert scale (McKeown, 2001). In particular, the sorting grid used in Q studies might feature progressive numbers (1–11), letters (A–K), or even emoticons, ranging from large smiles to expressions of severe disappointment. The main aim of these indicators is to facilitate participants' relational sorting of statements based on their personal views (Ho, 2017). However, each statement is assigned a score for statistical analysis purposes, but this scoring serves only this mathematical function. It's also important to note that the scores related to statement placement are significant for the individual participant. From the Q researchers' perspective, these scores cannot be used to fit the participants' choices into any predetermined interpretive model of them; they are only used to conduct the factor analysis.

Data Analysis

The collected Q sorts were analyzed by using the desktop version of the free software KADE v1.2.1 (Banasick, 2019).[2] The comments sorted by the participants supported the process of the viewpoints' definitions and interpretations. Seven participants' Q sorts (five from the computer science group and two from the psychology group) were not included in the calculation of the scores for each statement for the factor arrays, either due to high factor loadings (the measure for Q sort's correlation strength with the corresponding viewpoint) in more than one viewpoint, or they were not statistically significant at $p < 0.01$ (Brown, 1980, 1986).

The statistical analysis of the 46 Q sorts resulted in a three-viewpoint solution. Viewpoint # 1, interpreted as *Professionals*, included the cybersecurity instructor/expert, 15 computer science students, and 11 psychology students. Viewpoint # 2 was interpreted to be the *Skeptics*; it included two psychology students and two computer science students. The third viewpoint was interpreted as the *Personals* and was composed of eight psychology students (see Table 2).

[2] Factor extraction was run by applying principal component analysis (PCA) followed by Varimax rotation.

Table 2 Summary table of the participants contributing to each viewpoint

Participant status	*Professionals*	*Skeptics*	*Personals*
Expert	1	0	0
Psychology Major	11	2	8
Computer Science Major	15	2	0
Total	27	4	8

The Q sorts that populated each viewpoint and the corresponding factor loadings are shown in Appendix 3. The bold font and an X next to the factor loading value for any given Q sort specifies that the Q sort was used to define the viewpoint specified in the first row of the table (*Professional*, *Skeptics*, *Personals*). The factor arrays or composite factors for each viewpoint are shown in Appendix 2.

Results

The following findings emerged from the interpretation (Albright et al., 2020) of results as reported in the factor arrays.

Viewpoint #1. Professionals. This viewpoint could be interpreted along three main ideas:

(1) the *relevance* of cybersecurity in current times: cybersecurity is a problem for the entire community, rather than an issue for the single individual (for example, #32: **+4*D***, +2, +1. Note that # 32 refers to the statement; +4D, the first number of the string in bold, is the score that the *Professionals'* factor array has for the statement # 32, and it is a distinguishing *D* statement; +2 is the score for # 32 in the *Skeptics'* factor array, and +1 is the score in the *Personals'* factor array, #15: **+5**, +4, +3);

(2) *how* problems of cybersecurity can be effectively addressed:

(2a) Technical aspects. Focus should be put on technical aspects such as accepting the hassle of two-step authentication (#37: **+5**, -1 *D*, +5), or avoiding sharing information on social media (#33: **–5 *D***, -2, 0);

(2b) Education. There is a clear acknowledgment that everyone should learn how to protect themselves from cyber risks (#1: **+4 *D***, +1 *D*, +5 D);

(3) *who* should be the active agents in promoting effective cybersafe behaviors. The *agents* involved are:

(3a) employees, regardless of whether they operate as IT workers (#43: **-4 *D***, +2 *D*, -3 *D*), and

(3b) companies that should maintain robust cyber protocols (#31 C: **+4**, 5, 4).

In summary, the *Professionals* demonstrated a well-rounded approach to cybersecurity, including modern-day issues that can prioritized, suggesting solutions, and concluding with a discussion of who should do it. The emphasis of this viewpoint on training and learning highlights the importance of an advanced education, both technical and nontechnical. The expert/professor's opinion contributed to the characterization of this viewpoint. It is important to note that the participants from the computer science program demonstrated alignment with the expert/professor's opinion. It is interesting that a group of psychology students demonstrated a similar approach to cybersecurity, despite their lack of technical knowledge in computer science. These findings substantiate the utility of Q in allowing the identification of opinion groups comprising individuals not bonded to preconstitute categories—or background.

Viewpoint #2. Skeptics. This viewpoint demonstrated a focus on major cyberattacks that will be an inevitable part of future cyberspace (#11: +2, **+4**, 0 *D)*, and expressed concern pertaining to the practices of (1) US business and (2) the US government.

(1) U.S. business organizations are not considered able to handle attacks on their digital systems (#27: -3, **-4**, -2). This viewpoint indicated that the privacy settings on the web platforms are ineffective (#18: -2, **+5 *D***, -5 *D*), which implies the need for organizations to introduce and maintain robust cybersecurity protocols (#31 C: +4, **+5**, +4). One participant (33cscsn)[3] directly expressed this mistrust toward U.S. businesses, writing that ". . . companies don't really care about their users that much. They sell their own users' data just to make a profit, why would I trust them to make the best decisions regarding our data?"

(2) Beyond the communicated need for safer infrastructures, this group did not consider the U.S. government as capable of managing cybercrimes or protecting the data collected from the citizens (#19: -1 *D*, **-5 *D***, -2 *D*), (#40: 0, **+4 *D***, +1), (#23: -1, **-4 *D***, -3). This distrust was further highlighted by rejecting the possibility that the U.S. government can access encrypted communications when investigating crimes (#25: 0, **-5 *D***, -1), (#13: -1 *D*, **-4**, -4). This perspective was clearly communicated in the comment by participant 25cscsn, who wrote, "I am a strong believer in the Fourth Amendment, and I believe that lots of information that the government does harvest is not for the benefit of the general public. . . . I simply believe there are too many points of failure for the government to fully protect my data." In summary, the primary concerns regarding cybersecurity for the *Skeptics* were the inability of U.S. businesses to warrant adequate security when delivering their services to the clients, and likewise, a distrust in the U.S. government for not being able to prevent cybercrimes.

[3] To orient the reader: the number in front of a participant label is a progressive number, "csc" stands for "computer science student," "psy" stands for "psychology student." The suffix "sn" added to both refers to the fact that they are senior students.

Viewpoint #3. Personals. This group expressed an opinion that can be synthesized as cybersecurity being a personal issue that affects the personal life. They acknowledged the importance of learning how to protect their personal information (#1: +4 *D*, +1 *D,* ***+5 D***), and the utility of the elaborate cybersafe procedures such as the two-step authentication processes (#37: +5, -1 *D*, **+5**). This opinion however did not considered sharing of passwords with family and friends as a cyberhazard (#21: -2, -1, ***+4 D***), and did not fear losing control of one's personal information (#28: -1 *D*, 1 *D*, ***-4 D***). Participant 4psysn provided the following representative comment about sharing passwords:

> I think that people should learn how to trust people with their passwords, close friends, family members, just in case something comes up and they need to access your account, however it is also very important to know which information to give and which information to keep to yourself.

Where some experts may see this as an example of unsafe cyberbehaviors, this comment highlights what may indeed be a reasonable explanation for ordinary (non-expert) people in the context of the current highly digitalized society. Given that valuable pieces of personal information can be found online, it may become necessary to make them accessible to those who are closer in our social network (family members and trusted friends). Moreover, the abovementioned viewpoint expressed concern about the effort required to keep track of all the various passwords needed for the different online accounts (#46: -2 *D*, 2, ***4 D***). An example of this perspective was communicated by participant 21psysn in the following synopsis: "Sometimes I find it easier to set the same passwords because I always forget and then have to reset. And by making passwords easy to guess, it makes it a lot easier for bad things to happen."

In short, the *Personals* looked at the cybersecurity as an individual, personal issue or concern. They swung between the acknowledgment of the importance of getting appropriate education to protect one's personal information, or using the two-step authentication procedures and the rejection of these principles when declaring that the sharing one's passwords with family and friends is not a cyberrisk. They also swung back when expressing fear for the safety of the passwords used—a fear that, however, becomes less relevant when considering one's extensive response effort required to comply with the cybersecurity protocols.

The Consensus Statements

"Consensus is determined when a statement has similar (but not necessarily the same) grid positions between *pairs* of [viewpoints]" (Ramlo & Nicholas, 2020, p. 13, emphasis in original; Brown, 1980; McKeown & Thomas, 2013, Watts & Stenner, 2012). The three viewpoints shared consensus for several statements. One of these statements referred to the request directed to companies to adopt more robust cybersafe protocols (# 31: +4, +5, +4). Different reasons may explain such consensus among the three differentiated viewpoints. For the *Skeptics* (+ 5), it looks consistent with their skepticism about the organizations adopting such basic procedures to protect their clients. For the *Professionals* (+4), it matches their approach to cybersecurity that involves all the agents operating in society, including the private sector represented by the companies. For the *Personals* (+4), having companies that adopt more robust protocols might, possibly, decrease their concerns about their cybersafety. Such consensus aligned with the recent (September 2022) development of "State and Local Cybersecurity Grant Program" by Cybersecurity and Infrastructure Security Agency to help eligible entities to address cybersecurity risks (Cybersecurity & Infrastructure Security Agency, 2022).

Discussion

The purpose of this study was to provide, using the Q methodology, a systematic description of the viewpoints about cybersecurity-related opinions for college students, as part of a behavioral systemic analysis of problems that can emerge in a community, specifically with respect to the violations of the cybersecurity protocols. The Q methodology allowed the potential for alignment of viewpoints shared by psychology and computer science majors in relation to those offered by the expert/professor in cybersecurity.

Our findings refer to the emergence of three different viewpoints interpreted as *Professionals, Skeptics,* and *Personals*. As demonstrated by the data, differences in background did not prevent the computer science students and the psychology students from sharing their opinions on cybersecurity. The third viewpoint, the *Personals*, communicated only by students without formal education in computer science, showed an opinion about the risks in cyberspace as a personal, and often difficult experience to manage. These findings may have implications for the leadership communities that may recognize the importance of designing educational interventions consistent with the needs of both the next generations of cybersecurity experts and ordinary internet users.

The *Professionals* indicated that cybersecurity affects everyone and as such must be addressed by everyone, both experts and nonexperts in computer science and cybersecurity. This viewpoint demonstrated the necessity for clear and defined roles for individuals in companies, the government, and other organizational systems when it comes to mitigating cybersecurity threats. This is especially important from an educational perspective, because individuals, both as cybersecurity developers and final users, need to understand how their actions affect the safety of the cybersystem, and the society as a whole.

The *Skeptics* demonstrated a distrust for U.S. businesses and the U.S. government in contrasting the cybercriminal actions to protect their users. This opinion was communicated by both individuals with computer science and noncomputer-science backgrounds, hence showing that distrust was shared regardless of level of cybersecurity expertise.

The identification of the *Personals* viewpoint has important implications for cybersecurity, as this viewpoint was shared exclusively by individuals with a noncomputer-science background. Moreover, it emphasizes how one's personal experience, and values affect the adoption of correct cybersafe behaviors. They represent most of the internet users, and they are often pointed as the weak spot for the appropriate functioning of the cyberprocedures (Conteh & Schmick, 2016; Furnell & Clarke, 2012; McMahon, 2020; Moustafa et al., 2021; Sabillon et al., 2016, Salahdine & Kaabouch, 2019; Wang et al., 2020; Wiederhold, 2014).

Limitations and Extensions

In summary, this study aimed to explore how college students perceive the cybersafe use of internet services, extending the work of Ramlo and Nicholas (2020, 2021), who focused on cybersecurity experts and students in computer science and engineering. To diversify the P set for our Q study, we recruited psychology majors through an online platform facilitated by the university's psychology department. Although this method efficiently reached our target demographic, it limited our expanded P set to psychology students only. This limitation may restrict the possibility to ascertain whether students from varied disciplines—such as humanities, business, legal studies, and the natural sciences, to cite just a few—would express opinions similar to or distinct from those of computer science students, our reference group.

This narrow focus is particularly significant because one goal of the research was to establish a foundation for designing educational interventions addressing cybersecurity's social aspects from both user and developer perspectives, based on the perspectives of college students—rather than factors that often guide the public policy decisions (e.g., availability of resources in a wide sense). It is regrettable that constraints on time and resources precluded the broadening of our participant base. These observations suggest avenues for extending the research to include college students from varied experiences and backgrounds. It is important to note that within the Q methodology, comparisons focus on shared opinions emerged from the Q analysis as described, rather than demographic categories, distinguishing it from approaches like ANOVA that compares and looks for demographic differences.

Concerns may arise regarding the exclusive use of written stimuli in this Q study, particularly in terms of inclusivity for participants with varied reading abilities or visual impairments. It is reasonable to expect college students to possess adequate reading skills and, given the topic under investigation, familiarity with the use of the internet. However, disparities in educational backgrounds or visual challenges may necessitate alternative approaches, such as the utilization of auditory stimuli, to ensure broader participation. The use of auditory and visual stimuli poses, however, a potential experimental challenge pertaining to the interchangeability of the two types of stimuli. To address this challenge, a preliminary study could be designed by creating two different Q sets composed of stimuli with identical content but having a different format: visual and auditory. These would be sorted independently by a pilot group capable of accessing both modalities. Subsequent Q analysis (see, e.g., Brown, 1980, pp. 159–172; Brown, 1992; Brown & Feist, 1992; Coke & Brown, 1976; Ramlo, 2019; Rhoads & Brown, 2002; Sell & Craig, 1983; Wilson, 2006; Wingreen & Blanton, 2018) would assess if participants align with the same factors across both stimuli types. This approach directly tests the stimuli's interchangeability through participant interaction, rather than relying on researcher's assumptions.

Conclusion

Based on behavioral systemic approach to cultural change, innovation in education opportunities can benefit from (1) encouraging safe cybersecurity practice among the ordinary internet users with no computer science background, and (2) updating the training content of the cybersecurity developers so that they can understand the psychological, cultural and sociological factors that influence the behavior of their final users. Moreover, cybersecurity professionals need to make it more affordable for individuals to protect their personal information. The more difficult and time consuming safe cyberbehavior is, the less likely individuals are to practice it. This means that methods for data management need to be developed to make it easy for individuals to access their data without having to remember upwards of 20 different passwords. In addition, training for nonexperts in computer science that highlights the importance of keeping passwords and data secure, even from friends and family should be available to the public. These training sessions should be of high quality and easy to complete, as shown by the findings associated with the *Personals* perspective. For example, the consequences arising from identity thefts, ransomware (MacColl et al., 2024), and interruption of public services are often delayed and uncertain in their effects on the ordinary users' lives; thus, such users often dismiss these menaces as "occurring to someone else." As known from the experimental analysis of behavior, delayed and uncertain consequences have mild influence on the behavior (Rachlin, 1974, 2004; Rachlin & Green, 1972). In that regard, cyberrisks need to be communicated as high-probability threats, which can be avoided by learning—and applying—the appropriate strategies.

As we see it, the science of behavior can provide guidelines on ways to design training interventions that account for the psychological, cultural and sociological factors affecting human behavior. In that regard, trainings offered to the internet users, operating either as private individuals or as part of the organizations' non-IT workforce can be designed to favor (1) the discrimination of inappropriate cyberactions that are often made not easily avoided by the cybercriminals' attacks, and (2) the generalization of the appropriate cyberactions within new contexts. This can be achieved using realistic cyberscenarios and frequent and differentiated repetitions within varied environments that require physical interactions, rather than simply answering test questions.

With regard to the education of next generation of cybersecurity experts and developers, incorporation of information regarding human behavior across the following domains should relate to: (1) how the environmental context (the contextual set of physical stimuli) operates on people's behaviors; (2) how one's experience, the community culture, the current emotional and physical status, and the individual's future expectations can affect the users' behavior; (3) how different type of consequences (immediate, delayed, certain or uncertain) associated to the operations in the cyberspace can shape safe (or unsafe) cyberbehaviors; and finally, (4) under what circumstances the response effort to comply with designed cyberprotocols becomes so challenging that it is eventually dismissed or poorly implemented (Kantor, 1982; Skinner, 1953). In summary, the cyberexperts bear the responsibility to develop their cyberproducts accounting for the psychological aspects of their final, nontechnical users: it is worth reiterating that any tool is more effective the more its developers know and understand the behavior, the culture and the society of the users of their tools. It is should be noted that future Q studies can further guide the design of educational programs within the educational, government, and business sectors that aim to align with the evolving perspectives of their consumers (e.g., students, workers, and receivers of their products). The latter, then, can help to integrate and develop the education and training of cybersecurity experts and developers. Overall, continuous cybersecurity innovation as well as the advancement in cybersecurity education should ultimately be measured by the cybersafe behaviors of the users of associated technologies.

However, the effectiveness of the education subsystem's actions cannot be accomplished without an appropriate coordination with other subsystems composing the society, thus reiterating the necessity that social issues' analysis and corresponding intervention design and implementations (public choices) need a systemic approach grounded on the principles of behavior. Based on the literature in computer science, leaders have the fundamental responsibility to promote trust in institutions and the economic system because it affects the safety and quality of the supplier chain of goods and services. Such trust can be established, among other strategies, by adopting appropriate organizational policies. At the level of private business, companies need to invest more resources in their cybersecurity workforce and put protocols in place to protect their users' data. The governments (the U.S. government in our study) need to enforce cybersafe behavior at the public policy level. Moreover, there is also a need for more incentives (in a wide sense) for cybersecurity professionals to work in government settings. As the salaries from private industries are quite competitive, qualified professionals are often dissuaded from working within the federal government, where their skills could assist in implementing these policies and consequently protecting the people from cybercrime.

Furthermore, behavior analytic research with a focus on behavioral systemic applications may benefit from using Q methodology as an assessment mechanism to demonstrate the impact of interventions and training programs on opinions of the community of recipients throughout the research process (e.g., pre- and post-exposure to interventions or training programs). These studies may also include comparative analyses across different communities (Akhtar-Danesh & Wingreen, 2022; Brown, 1980, Coke & Brown, 1976; Davies & Hodge, 2012; Klaus et al., 2010; Ramlo, 2015, 2019; Sell & Craig, 1983; Wilson, 2006; Wingreen & Blanton, 2018).

Q methodology may also inform behavior analytic studies of social validity. Social validity is a term used in behavior science to refer to the social importance and acceptability of treatment goals, procedures, and outcomes (Baer et al., 1968; Hawkins, 1991; Wolf, 1978). Wolf (1978) and Hawkins (1991) explored social validity and functional assessment of the societal importance of the goals, technologies, procedures, and affects achieved by applications of behavior analysis. Their analyses consider the social validity of interventions applied to help special needs populations and provide a framework to consider the impact of behavior science on larger social issues (Baer et al., 1968). For instance, Hawkins (1991) provides an overview of habilitative validity, which encompasses stakeholders' (including caregivers and care providers) engagement in the development and review of objectives, procedures, and outcomes of selected.

As highlighted by Alderson et al. (2018),

> . . . putting new policies into place requires knowledge of the context, including how a given policy will fit with stakeholder values. Assuming that the basic resources are available, the main stumbling blocks to policy implementation often include the . . . behaviors of key interested parties—those responsible for delivering the policy and those in the target population whose cooperation is required for its success (the policy stakeholders). (p. 737)

In short, Q offers informative analyses associated with many viewpoints that are more detailed than simple averages from predefined categories. Even more interesting, from a leadership point of view, Q identifies consensus areas among the different perspectives on which action plans can be more successfully implemented (van Eeten, 2001). Success, of course, is measured in units important to the organizations, and outcome data that can be used to validate the utility of the Q results.

To conclude, the Q approach can be a useful tool for understanding different viewpoints in the analysis and design of organizational policies and rules. In addition, the analytical perspective offered by Q provides ways to enhance social validity of organizational, and community interventions from employees, citizens, and consumer standpoints. In that regard, there is an evolving line of research (Baker & van Exel, 2022; Baker et al., 2010, 2014; Brown, 2002b; Talbott, 1963/2010; van Exel et al., 2006, 2007, 2008) that it is aimed at utilizing Q results to inform design and administration of polling mechanisms among large samples of people across communities. This approach has the value adding potential for expanding behavior scientific analysis of leadership decision making, and the influence of organizational practices on cultural change (Houmanfar & Rodrigues, 2006; Houmanfar et al., 2009, 2010; Houmanfar & Szarko, 2022). Moreover, it can contribute to the expansion of the analytical tools available for the culturo-behavioral scientists and practitioners.

Appendix 1

Demographics of the Participants

Table 3 Age of the participants in the study

Group	*N*	18-25	26-35	36-45	+45
Psychology Major	23	20	2	1	0
Computer Science Major & the expert	23	17	4	1	1
All participants	46	37	6	2	1

Table 4 Gender of the participants in the study

Group	*N*	Female	Male	Other
Psychology Major	23	17	6	0
Computer Science Major & the expert	23	3	20	0
All participants	46	20	26	0

Table 5 Citizenship of the participants in the study

Group	*N*	US citizen	International
Psychology Major	23	23	0
Computer Science Major & the expert	23	22	1
All participants	46	45	1

Appendix 2

Factor Array Positions for the Three Viewpoints

Statement Number	Statement	*Professionals*	*Skeptics*	*Personals*
1	It is important for everyone to learn how to protect their own personal information	4 *D*	1 *D*	5 *D*
2	Screen locks or other security features to access my phone are a nuisance	-4 *D*	-2 *D*	-5 *D*
3	I feel that it is safe to utilize public WiFi networks for tasks like online banking or e-commerce	-5	-3	-1 *D*
4	It is relatively easy for hackers to infiltrate electronic devices on public WiFi sources like those found in places like coffee shops	1 *D*	-1	-1

Statement Number	Statement	*Professionals*	*Skeptics*	*Personals*
5 **C**	I feel like I am knowledgeable about cybersecurity and preventing a cyberattack on my electronic devices	0	0	-2
6	Cyberattacks and data breaches are facts of life for government agencies, businesses and individuals.	3	2	1
7 **C**	I do not trust social media organizations to protect my personal data	3	3	2
8	I frequently neglect cybersecurity best practices	-3 *D*	0	0
9 **C**	I need cybersecurity training so that I better understand how minor mistakes or simple oversights might lead to a disastrous scenario regarding the security or bottom line of my organization	1	0	1
10	I feel that the US government is at least somewhat prepared to handle cyberattacks on our public infrastructure.	0	-1	-1
11	Major cyberattacks will be a fact of life in the future	2	4	0 *D*
12 **C**	Technology companies should be able to use encryption tools that are unbreakable even to law enforcement	0	1	0
13	The US government should be able to access encrypted communications	-1 *D*	-4	-4
14	Everyone who uses a computer or smartphone should learn about cybersecurity	2	-1 *D*	3
15	It is important to keep critical infrastructure from cyber threats	5	4	3
16	You should wait to install updates to your operating system, browser, and other critical software until you hear the "bugs" have been worked out	-1	1	-1
17 **C**	I don't see a problem using a social media platform such as Facebook to log in to a third-party site	-3	-3	-2
18	Privacy settings on social media and other web-platforms are meaningless	-2 *D*	5 *D*	-5 *D*
19	The US government is prepared to handle future cyberattacks	-1 *D*	-5 *D*	-2 *D*
20	It is easy to become a victim of an email phishing campaign or other social engineering attack	1	1	- 3 *D*
21	Sharing passwords with a friend or family member is ok if they are trustworthy	-2	-1	4 *D*
22	I do not worry about how secure my online passwords are	-3	-2	-4
23	I trust the federal government to protect my personal data	-1	-4 *D*	-3
24	I don't see a problem using the same password for different accounts. What's the big deal?	-4 *D*	0	-1
25	The government should be able to access encrypted communications when investigating crimes	0	-5 *D*	-1
26	I feel that I am careful about how I use the internet and electronic devices	1	1	3

Statement Number	Statement	*Professionals*	*Skeptics*	*Personals*
27	I feel confident that US businesses are prepared to handle attacks on their own systems	-3	-4	-2
28	I fear I have lost control of my personal information	-1 *D*	1 *D*	-4 *D*
29 **C**	Every time we connect to the Internet, we make decisions that affect our cybersecurity	2	0	2
30 **C**	Passwords are the first line of defense against unauthorized access to user data so I take them very seriously	2	3	3
31 **C**	Companies should maintain robust protocols when it comes to cybersecurity	4	5	4
32	Cybersecurity is considered one of the key national security issues of our time	4 *D*	2	1
33	Sharing personal information on social media, like your birthdate or best friend's name, is not a threat to your personal cybersecurity	-5 *D*	-2	0
34	The private sector is prepared to handle future cyberattacks	-2	-3	-2
35 **C**	It is important to set strong passwords, change them regularly, and not share them with anyone	3	3	2
36	Our daily life, economic vitality, and national security depend on a stable, safe, and resilient cyberspace	3	0	2
37	It's worth the hassle to use two-step authentication on at least some of my online accounts	5	-1 *D*	5
38	There aren't many careers left that aren't based on technology	-1 *D*	2	1
39	Cyber attackers rely on human error	1	-2 *D*	0
40	I worry whether government agencies and major corporations can protect the customer data they collect.	0	4 *D*	1
41 **C**	Security know-how can advance you in your existing job	1	-1	2
42	It's a bad idea to write down your passwords on paper	0 *D*	-2	-3
43	With attacks becoming more advanced and sophisticated, employee training in cybersecurity is nearly pointless unless you work in IT.	-4 *D*	2 *D*	-3 *D*
44	I feel like password management is a stressful and uncertain process	-2	-3	1 *D*
45	My personal data has become less secure in recent years	0	3	0
46	It's challenging to keep up with all of the passwords to my various online accounts	-2 *D*	2 *D*	4 *D*
47	It's a bad idea to have passwords containing wholewords, part of your phone number, etc.	2	0	0

The table reports for each statement their position scores on the corresponding factor array. Consensus statements and Distinguishing statements (at $p < 0.01$) are indicated respectively with a C (in bold) next to the statement number, and a D (in italics) next to the position score on the grid

Appendix 3

Factor Matrix of the Three Viewpoints

Q sort	Participant status	*Professionals*	*Skeptics*	*Personals*
1	Expert	**0.7799X**	0.2744	0.1993
3	Psychology student	**0.5756X**	-0.2167	0.1476
6	Psychology student	**0.6085X**	0.369	0.1698
9	Psychology student	**0.4834X**	0.2682	0.3032
10	Psychology student	**0.6155X**	0.4068	0.2605
12	Psychology student	**0.5489X**	-0.1931	0.3759
14	Psychology student	**0.5604X**	0.0584	-0.0173
15	Psychology student	**0.5235X**	0.414	0.3043
16	Psychology student	**0.5776X**	-0.1797	0.2382
17	Psychology student	**0.486X**	0.1746	0.1445
20	Psychology student	**0.6625X**	0.054	0.4426
22	Psychology student	**0.4827X**	0.0766	0.4584
27	Computer science student	**0.6226X**	0.4262	0.252
28	Computer science student	**0.6817X**	0.2894	0.0061
30	Computer science student	**0.6987X**	0.3581	0.2883
31	Computer science student	**0.5552X**	0.4058	0.1847
32	Computer science student	**0.6331X**	0.431	0.1859
34	Computer science student	**0.7098X**	-0.145	-0.1375
35	Computer science student	**0.7518X**	0.2591	-0.0012
36	Computer science student	**0.7924X**	-0.1129	0.3919
40	Computer science student	**0.8067X**	0.2313	0.1387
41	Computer science student	**0.615X**	0.3904	0.2177
42	Computer science student	**0.6039X**	0.1567	0.4377
43	Computer science student	**0.5287X**	0.0311	0.4942
44	Computer science student	**0.594X**	-0.0395	0.4091
45	Computer science student	**0.5502X**	0.4403	0.3755
46	Computer science student	**0.7695X**	0.1619	0.2239
7	Psychology student	-0.0233	**0.5766X**	-0.1422
24	Psychology student	0.2688	**0.6569X**	0.2059
25	Computer science student	0.3583	**0.5352X**	0.1969
33	Computer science student	0.0246	**0.7311X**	0.3416
2	Psychology student	-0.0956	0.2334	**0.6056X**
4	Psychology student	0.2341	-0.35	**0.4998X**
8	Psychology student	0.4469	0.0862	**0.5802X**
11	Psychology student	0.468	0.0105	**0.6156X**
13	Psychology student	0.1872	-0.0566	**0.6405X**
18	Psychology student	0.1974	0.1257	**0.5264X**
21	Psychology student	0.0789	0.1306	**0.4113X**

Q sort	Participant status	*Professionals*	*Skeptics*	*Personals*
23	Psychology student	0.053	0.0365	**0.545X**
5	Psychology student	0.099	0.1459	-0.1098
19	Psychology student	-0.0159	-0.3866	0.054
26	Computer science student	-0.0065	0.0658	-0.0051
37	Computer science student	0.3679	0.3927	0.321
29	Computer science student	0.1558	0.3229	0.18
38	Computer science student	0.2313	0.5837	0.5541
39	Computer science student	0.447	0.3682	0.298

The factor loading in bold font and with an X for a given Q sort indicates that it contributes to the definition of the factor arrays

Acknowledgements We thank Dr. Diane Montgomery for her support and directions pertaining to the Q sort analysis, and Dr. Mark Alavosius for his informative suggestions throughout the publication process.

Authors' Contributions Rita Olla (Author #1) played a pivotal role in establishing the methodology, data collection, analysis, and interpretation. As the first author, she generated the first draft and conducted the revisions throughout the manuscript development process. Ramona A. Houmanfar (Author #2) provided project supervision, contributed to the development of manuscript, and guided the editorial process. Shamik Sengupta (Author #3) contributed to the content in the introduction section of the manuscript and offered editorial support during the editorial process. Emily M. Hand (Author #4) contributed to the development of the discussion section and editorial process. Lastly, Sushil J. Louis (Author #5) offered support throughout the editorial process.

Funding The authors would like to acknowledge the National Science Foundation for grant n. 2121559, which made this research possible. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the view of the National Science Foundation.

Data Availability The dataset analyzed in the current study is available from the corresponding author on reasonable request.

Declarations

Ethical Approval All procedures performed in studies involving human participants were in accordance with the ethical standards of the institutional and/or national research committee and with the 1964 Helsinki declaration and its later amendments or comparable ethical standards.

Informed Consent Informed consent was obtained from all individual participants included in the study.

Conflict of Interest The authors declare that they do not have any conflict of interest.

References

Adcock, C. J. (1954). *Factorial analysis for non-mathematicians*. Melbourne University Press.

Akhtar-Danesh, N., & Wingreen, S. C. (2022). How to analyze change in perception from paired Q-sorts. *Communications in Statistics-Theory and Methods, 51*(16), 5681–5691. https://doi.org/10.1080/03610926.2020.1845734

Alavosius, M. P., Houmanfar, R. A., Anbro, S., Burleigh, K., & Hebein, C. (2017). Leadership and crew resource management in high-reliability organizations: A competency framework for measuring behaviors. *Journal of Organizational Behavior Management, 37*, 142–170. https://doi.org/10.1080/01608061.2017.1325825

Albright, E. A., Christofferson, K., McCabe, A., & Montgomery, D. (2020). Lessons learned: Some guidelines to factor interpretation. *Operant Subjectivity*, *41*, 1–13. https://ojs.library.okstate.edu/osu/index.php/osub/article/view/8683

Alderson, S., Foy, R., Bryant, L., Ahmed, S., & House, A. (2018). Using Q-methodology to guide the implementation of new healthcare policies. *BMJ Quality & Safety, 27*(9), 737–742. https://doi.org/10.1136/bmjqs-2017-007380

Aljuaid, A., & Liu, X. M. (2023). Sociocultural barriers for female participation in STEM: A case of Saudi women in cybersecurity. *Journal of Cybersecurity Education: Research & Practice*, *2023*(1), Article 2. https://digitalcommons.kennesaw.edu/jcerp/vol2023/iss1/2

Baer, D. M., Wolf, M. M., & Risley, T. R. (1968). Some current dimensions of applied behavior analysis. *Journal of Applied Behavior Analysis, 1*(1), 91–97.

Baker, R. M., & van Exel, J. (2022). Q methodology and questionnaire. In J. C. Rhoads, D. B. Thomas, & S. R. Ramlo (Eds.), *Cultivating Q methodology. Essays honoring Steven R. Brown* (pp. 298–313). International Society for the Scientific Study of Subjectivity.

Baker, R. M., van Exel, J., Mason, H., & Stricklin, M. (2010). Connecting Q & surveys: Three methods to explore factor membership in large samples. *Operant Subjectivity, 34*(1), 38–58. https://doi.org/10.15133/j.os.2010.003

Baker, R., Wildman, J., Mason, H., & Donaldson, C. (2014). Q-ing for health—A new approach to eliciting the public's views on health care resource allocation. *Health Economics, 23*(3), 283–297. https://doi.org/10.1002/hec.2914

Banasick, S. (2019). KADE: A desktop application for Q methodology. *Journal of Open Source Software, 4*(36), 1360. https://doi.org/10.21105/joss.01360

Brethower, D. M. (1982). The total performance system. In R. M. O'Brien, A. M. Dickinson, & M. P. Rosow (Eds.), *Industrial behavior modification: A management handbook* (pp. 350–369). Pergamon Press.

Brethower, D. M. (1999). General systems theory and behavioral psychology. In H. D. Stolovitch & E. J. Keeps (Eds.), *Handbook of human performance technology* (pp. 67–81). Jossey-Bass Pfeiffer.

Brethower, D. M. (2000). A systematic view of enterprise: Adding value to performance. *Journal of Organizational Behavior Management, 20*, 165–190. https://doi.org/10.1300/J075v20n03_06

Brewer-Deluce, D., Sharma, B., Akhtar-Danesh, N., Jackson, T., & Wainman, B. C. (2020). Beyond average information: How Q-methodology enhances course evaluations in anatomy. *Anatomical Sciences Education, 13*(2), 137–148. https://doi.org/10.1002/ase.1885

Brown, S. R. (1980). *Political subjectivity. Applications of Q methodology in political science*. Yale University Press.

Brown, S. R. (1986). Q technique and method. Principles and procedures. In W. D. Berry & M. S. Lewis-Beck (Eds.), *New tools for social scientists: Advances and applications in research methods* (pp. 57–76). Sage.

Brown, S. R. (1992). Expositor: A note on measuring changes in Q factor loadings. *Operant Subjectivity*, *15*(2), 56–61. https://ojs.library.okstate.edu/osu/index.php/osub/article/view/9041

Brown, S. R. (1993). A primer on Q methodology. *Operant Subjectivity, 16*(3/4), 91–138. https://doi.org/10.15133/j.os.1993.002

Brown, S. R. (1994). Q methodology and interbehavioral phenomenology. *The Interbehaviorist, 22*(3), 24–26.

Brown, S. R. (1999). On the taking of averages: Variance and factor analyses compared. *Operant Subjectivity*, *22*(3), 31–37. https://ojs.library.okstate.edu/osu/index.php/osub/article/view/8963

Brown, S. R. (2002a). Subjective behavior analysis. *Operant Subjectivity*, *25*(3/4), 148–163. https://ojs.library.okstate.edu/osu/index.php/osub/article/view/8909

Brown, S. R. (2002b). Q technique and questionnaires. *Operant Subjectivity*, *25*(2), 117–126. https://ojs.library.okstate.edu/osu/index.php/osub/article/view/8914

Brown, S. R. (2006). Q methodology and naturalistic subjectivity. In B. D. Midgley & E. K. Morris (Eds.), *Modern perspectives on J. R. Kantor and interbehaviorism* (pp. 251–268). Context Press.

Brown, S. R. (2016). More than just a research tool: A comment on "An Overview of the Statistical Techniques in Q Methodology." *Operant Subjectivity*, *38*(3–4), 37–41. https://ojs.library.okstate.edu/osu/index.php/osub/article/view/8731

Brown, S. R. (2019). Subjectivity in the human sciences. *The Psychological Record, 69*, 565–579. https://doi.org/10.1007/s40732-019-00354-5

Brown, S. R., & Feist, U. (1992). Calibrating bilingual Q samples. *Operant Subjectivity*, *15*(4). https://ojs.library.okstate.edu/osu/index.php/osub/article/view/9033

Brown, S. R., & Melamed, L. E. (1990). *Experimental design and analysis*. Sage.

Brown, S. R., Durning, D. W., & Selden, S. C. (2007). Q methodology. In G. J. Miller & K. Yang (Eds.), *Handbook of research methods in public administration* (pp. 722–763). CRC Press/Taylor & Francis Group.

Brown, S. R., Baltrinic, E., & Jencius, M. (2019). From concourse to Q sample to testing theory. *Operant Subjectivity, 41*, 93–109. https://doi.org/10.22488/okstate.20.100582

Buehner, T. (2011). College student preferences for trendy versus classic typefaces. *Operant Subjectivity, 35*(1), 1–36. https://doi.org/10.15133/j.os.2011.001

Burt, C., & Stephenson, W. (1939). Alternative views on correlations between persons. *Psychometrika, 4*(4), 269–281. https://doi.org/10.1007/BF02287939

Coke, J. G., & Brown, S. R. (1976). Public attitudes about land use policy and their impact on state policy-makers. *Publius: The Journal of Federalism*, *6*(1), 97–134. https://www.jstor.org/stable/3329607

Conteh, N. Y., & Schmick, P. J. (2016). Cybersecurity: Risks, vulnerabilities and countermeasures to prevent social engineering attacks. *International Journal of Advanced Computer Research, 6*(23), 31–38. https://doi.org/10.19101/IJACR.2016.623006

Cusak, A. (2023). Case study: The impact of emerging technologies on cybersecurity education and workforces. *Journal of Cybersecurity Education, Research & Practice*, *2023*(1), Article 3. https://digitalcommons.kennesaw.edu/jcerp/vol2023/iss1/3

Cybersecurity & Infrastructure Security Agency. (2022). *State and local cybersecurity grant program*. https://www.cisa.gov/state-and-local-cybersecurity-grant-program

Davies, B. B., & Hodge, I. D. (2012). Shifting environmental perspectives in agriculture: Repeated Q analysis and the stability of preference structures. *Ecological Economics, 83*, 51–57. https://doi.org/10.1016/j.ecolecon.2012.08.013

Delprato, D. J., & Brown, S. R. (2002). Q methodology and the operant construct. *Operant Subjectivity*, *25*(3/4), 139–147. https://ojs.library.okstate.edu/osu/index.php/osub/article/view/8908

Delprato, D. J., & Knapp, J. R. (1994). Q methodology and interbehavioral description. *The Interbehaviorist, 22*(3), 14–23.

Duan, R., Hepworth, K., Ormerod, K. J., & Canon, C. (2021). Promoting concern for climate change: A study of wildfire photographs using Q methodology. *Science Communication, 43*, 624–650. https://doi.org/10.1177/10755470211041689

Durning, D. W., & Brown, S. R. (2006). Q methodology and decision making. In G. M. Morçöl (Ed.), *Handbook of decision making* (pp. 537–563). CRC Press/Taylor & Francis Group.

Fairweather, J. R., & Swaffield, S. R. (2002). Visitors' and locals' experiences of Rotorua, New Zealand: An interpretative study using photographs of landscapes and Q method. *International Journal of Tourism Research, 4*(4), 283–297. https://doi.org/10.1002/jtr.381

Fisher, R. A. (1971). *The design of experiments* (9th ed.). Collier Macmillan.

Foxall, G. R. (1999). The behavioural perspective model: Consensibility and consensuality. *European Journal of Marketing, 33*(5/6), 570–596. https://doi.org/10.1108/03090569910262143

Foxall, G. R. (2001). Foundations of consumer behaviour analysis. *Marketing Theory, 1*(2), 165–199. https://doi.org/10.1177/147059310100100202

Foxall, G. R. (2010). Invitation to consumer behavior analysis. *Journal of Organizational Behavior Management, 30*(2), 92–109. https://doi.org/10.1080/01608061003756307

Foxall, G. R. (2015). Consumer behavior analysis and the marketing firm: Bilateral contingency in the context of environmental concern. *Journal of Organizational Behavior Management, 35*(1/2), 44–69. https://doi.org/10.1080/01608061.2015.1031426

Freeze, D. (2022, January 22). 2022 cybersecurity almanac: 100 facts, figures, predictions and statistics. *Cybercrime Magazine*. https://cybersecurityventures.com/cybersecurity-almanac-2022/

Furnell, S., & Clarke, C. (2012). Power to the people? The evolving recognition of human aspects of security. *Computers & Security, 31*, 983–988. https://doi.org/10.1016/j.cose.2012.08.004

Glenn, S. S. (2004). Individual behavior, culture, and social change. *The Behavior Analyst, 27*(2), 133–151. https://doi.org/10.1007/BF03393175

Glenn, S. S., & Malott, M. M. (2004). Complexity and selection: Implications for organizational change. *Behavior & Social Issues, 13*, 89–106. https://doi.org/10.5210/bsi.v13i2.378

Hantula, D. A., DiClemente, D. F., & Rajala, A. K. (2001). Outside the box: The analysis of consumer behavior. In L. Hayes, J. Austin, R. Houmanfar, & M. Clayton (Eds.), *Organizational change* (pp. 203–223). Context Press.

Hawkins, R. (1991). Is social validity what we are interested in? Argument for a functional approach. *Journal of Applied Behavior Analysis, 24*, 205–213. https://doi.org/10.1901/jaba.1991.24-205

Hempel, A. C. (2021). Using visual Q-methodology to explore Danish children's outdoor play preferences. *Children, Youth & Environments, 31*(1), 88–115. https://doi.org/10.7721/chilyoutenvi.31.1.0088

Ho, G. W. (2017). Examining perceptions and attitudes: A review of Likert-type scales versus Q-methodology. *Western Journal of Nursing Research, 39*(5), 674–689. https://doi.org/10.1177/01939459166613

Houmanfar, R., & Rodrigues, N. J. (2006). The metacontingency and the behavioral contingency: Points of contact and departure. *Behavior & Social Issues, 15*, 13–30. https://doi.org/10.5210/bsi.v15i1.342

Houmanfar, R. A., & Szarko, A. (2022). Utilizing values-based governance to promote well-being in organizations and beyond. In R. A. Houmanfar, M. Fryling, & M. P. Alavosius (Eds.), *Applied behavior science in organizations: Consilience of historical and emerging trends in organizational behavior management* (pp. 291–315). Taylor & Francis Group.

Houmanfar, R. A., Rodrigues, N. J., & Smith, G. S. (2009). Role of communication networks in behavioral systems analysis. *Journal of Organizational Behavior Management, 29*, 257–275. https://doi.org/10.1080/01608060903092102

Houmanfar, R. A., Rodrigues, N. J., & Ward, T. A. (2010). Emergence and metacontingency: Points of contact and departure. *Behavior & Social Issues, 19*, 53–78. https://doi.org/10.5210/bsi.v19i0.3065

Houmanfar, R. A., Alavosius, M. P., Morford, Z. H., Herbst, S. A., & Reimer, D. (2015). Functions of organizational leaders in cultural change: Financial and social well-being. *Journal of Organizational Behavior Management, 35*, 4–27. https://doi.org/10.1080/01608061.2015.1035827

Kantor, J. R. (1982). *Cultural psychology*. Principia Press.

Kinsey, D. F. (1993). Humor communicability. *Operant Subjectivity, 17*(1/2), 49–61. https://doi.org/10.15133/j.os.1993.009

Klaus, T., Wingreen, S. C., & Blanton, J. E. (2010). Resistant groups in enterprise system implementations: A Q-methodology examination. *Journal of Information Technology, 25*(1), 91–106. https://doi.org/10.1057/jit.2009.7

Kline, P. (1994). *An easy guide to factor analysis*. Routledge.

Krapfl, J. E., & Gasparotto, G. (1982). Behavioral systems analysis. In L. W. Fredericksen (Ed.), *Handbook of organizational behavior management.* Wiley.

Kuipers, G., Sezneva, O., & Halauniova, A. (2022). Culture beyond words: Using visual Q-methodology to study aesthetic meaning-making. *Poetics, 91*, 101655. https://doi.org/10.1016/j.poetic.2022.101655

Lovie, P., & Lovie, A. D. (1996) Charles Edward Spearman, F. R. S. (1863–1945). *Notes & Records of the Royal Society of London*, *50*(1), 75–88. https://doi.org/10.1098/rsnr.1996.0007

MacColl, J., Hüsch, P., Mott, G., Sullivan, J., Nurse, J. R. C., Turner, S., & Pattnaik, N. (2024). The scourge of ransomware: Victim insights on harms to individuals, organisations and society. *Royal United Services Institute for Defence and Security Studies (RUSI) Occasional Paper*. https://static.rusi.org/ransomware-harms-op-january-2024.pdf

Malott, M. E. (2003). *Paradox of organizational change: Engineering organizations with behavioral systems analysis*. Context Press.

Malott, M. E. (2022). Paradox of organizational change: A selectionist approach to improving complex systems. In R. A. Houmanfar, M. Fryling, & M. P. Alavosius (Eds.), *Applied behavior science in organizations: Consilience of historical and emerging trends in organizational behavior management* (pp. 129–160). Taylor & Francis Group.

Malott, M. E., & Glenn, S. S. (2006). Targets of interventions in cultural and behavioral change. *Behavior & Social Issues, 15*, 31–56. https://doi.org/10.5210/bsi.v15i1.344

Mawhinney, T. C. (1992). Evolution of organizational cultures as selection by consequences: The Gaia hypothesis, metacontingencies, and organizational ecology. In T. C. Mawhinney (Ed.), *Organizational culture, rule-governed behavior and organizational behavior management* (pp. 1–26). Haworth Press.

Maxwell, J., & Brown, S. R. (1999). Identifying problems and generating solutions under conditions of conflict. *Operant Subjectivity, 23*(1), 31–51. https://doi.org/10.15133/j.os.1999.008

McKeown, B. (2001). Technical research note: Loss of meaning in Likert scaling: A note on the Q methodological alternative. *Operant Subjectivity*, *24*(4), 201–206. https://ojs.library.okstate.edu/osu/index.php/osub/article/view/8930

McKeown, B., & Thomas, D. B. (2013). *Q methodology* (2nd ed.). Sage.

McMahon, C. (2020). In defence of the human factor. *Frontiers in Psychology, 11*, 1390. https://doi.org/10.3389/fpsyg.2020.01390

Midgley, B. D. (2005). Unacknowledged behaviorist: An appreciation of William Stephenson's "Postulates of Behaviorism." *Operant Subjectivity, 29*(1/2), 87–93. https://doi.org/10.15133/j.os.2005.012

Midgley, B. D., & Delprato, D. J. (2017). Stephenson's subjectivity as naturalistic and understood from a scientific perspective. *The Psychological Record, 67*, 587–596. https://doi.org/10.1007/s40732-017-0258-8

Midgley, B. D., & Morris, E. K. (2002). Subjectivity and behaviorism: Skinner, Kantor, and Stephenson. *Operant Subjectivity, 25*(3/4), 127–138. https://doi.org/10.15133/j.os.2002.009

Moustafa, A. A., Bello, A., & Maurushat, A. (2021). The role of user behaviour in improving cyber security management. *Frontiers in Psychology, 12*, 561011. https://doi.org/10.3389/fpsyg.2021.561011

Olmstead, K., & Smith, A. (2017). Americans and cybersecurity. *Pew Research Center*. https://www.pewresearch.org/internet/2017/01/26/americans-and-cybersecurity/

Rachlin, H. (1974). Self-control. *Behaviorism*, *2*(1), 94–107. https://www.jstor.org/stable/27758811

Rachlin, H. (2004). *The science of self-control*. Harvard University Press.

Rachlin, H., & Green, L. (1972). Commitment, choice and self-control. *Journal of the Experimental Analysis of Behavior, 17*(1), 15–22. https://doi.org/10.1901/jeab.1972.17-15

Ramlo, S. E. (2015). Q methodology as a tool for program assessment. *Mid-Western Educational Researcher*, *27*(3). 207–223. https://scholarworks.bgsu.edu/mwer/vol27/iss3/3

Ramlo, S. E. (2019). Examining urban, American, middle-school students' divergent views of nature before and after a field trip to a university field station and nature preserve. *The Urban Review, 51*(2), 231–246. https://doi.org/10.1007/s11256-018-0473-x

Ramlo, S. E. (2022). A science of subjectivity. In J. C. Rhoads, D.B. Thomas, & S. E. Ramlo (Eds.), *Cultivating Q methodology. Essays honoring Steven R. Brown*. (pp. 182–216). International Society for the Scientific Study of Subjectivity.

Ramlo, S. E., & Nicholas, J. B. (2020). Divergent student views of cybersecurity. *Journal of Cybersecurity Education: Research & Practice*, *2019*(2), Article 6. https://digitalcommons.kennesaw.edu/jcerp/vol2019/iss2/6

Ramlo, S. E., & Nicholas, J. B. (2021). The human factor: Assessing individuals' perceptions related to cybersecurity. *Information & Computer Security, 29*(2), 350–364. https://doi.org/10.1108/ICS-04-2020-0052

Rhoads, J. C. (2001). Researching authoritarian personality with Q methodology Part I: Revisiting traditional analysis. *Operant Subjectivity, 24*, 68–85.

Rhoads, J. C., & Brown, S. R. (2002). "Sex, lies, and videotape": Attitudes toward the Clinton impeachment. *Operant Subjectivity*, *25*(2), 99–116. https://ojs.library.okstate.edu/osu/index.php/osub/article/view/8915

Rhoads, J. C., & Sun, T. W. (1994). Studying authoritarianism: Toward an alternative methodology. *Southeastern Political Review, 22*(1), 159–170.

Robertson, J., & Chapa, S. (2022). Hackers targeted US LNG producers in run-up to Ukraine war. https://www.bloomberg.com/news/articles/2022-03-07/hackers-targeted-u-s-lng-producers-in-run-up-to-war-in-ukraine

Robinson, T., Callahan, C., & Evans, K. (2014). Why do we keep going back? A Q method analysis of our attraction to horror movies. *Operant Subjectivity, 37*(1/2), 41–57. https://doi.org/10.15133/j.os.2014.004

Rummler, G. A. (2001). Performance logic: The organization performance Rosetta stone. In L. J. Hayes, J. Austin, R. Houmanfar, & M. C. Clayton (Eds.), *Organizational change* (pp. 111–132). Context Press.

Rummler, G. A., & Brache, A. P. (1995). *Improving performance: How to manage the white space on the organizational chart* (2nd ed.). Jossey-Bass.

Sabillon, R., Cavaller, V., Cano, J., & Serra-Ruiz, J. (2016). Cybercriminals, cyberattacks and cybercrime. *2016 IEEE International Conference on Cybercrime & Computer Forensic (ICCCF), Vancouver, Canada* (pp. 1–9). https://doi.org/10.1109/ICCCF.2016.7740434

Salahdine, F., & Kaabouch, N. (2019). Social engineering attacks: A survey. *Future Internet, 11*(4), 89.

Sell, D. K., & Craig, R. B. (1983). The use of Q methodology to investigate attitude change in American students who participate in foreign study programs: A review of the literature. *Operant Subjectivity*, *7*(1), 14–29. https://ojs.library.okstate.edu/osu/index.php/osub/article/view/9215

Simpson, S. H. (1989). Use of Q-sort methodology in cross-cultural nutrition and health research. *Nursing Research, 38*(5), 289.

Skinner, B. F. (1938). *The behavior of organisms*. D. Appleton-Century.

Skinner, B. F. (1953). *Science and human behavior*. Macmillan.

Skinner, B. F. (1965). Review lecture: The technology of teaching. *Proceedings of the Royal Society of London. Series B. Biological Sciences, 162*(989), 427–443.

Skinner, B. F. (1968). *The technology of teaching*. Appleton-Century-Crofts.

Somerstein, R. (2014). The taste test: Applying Q methodology to aesthetic preference. *Operant Subjectivity, 37*(1/2), 72–96. https://doi.org/10.15133/j.os.2014.006

Stephenson, W. (1935a). Correlating persons instead of tests. *Journal of Personality, 4*, 17–24. https://doi.org/10.1111/j.1467-6494.1935.tb02022.x

Stephenson, W. (1935b). Technique of factor analysis. *Nature, 136*(3434), 297–297. https://doi.org/10.1038/136297b0

Stephenson, W. (1936). Introduction to inverted factor analysis, with some applications to studies in Orexis. *Journal of Educational Psychology, 27*(5), 353–367. https://doi.org/10.1037/h0058705

Stephenson, W. (1953a). *The study of behavior*. University of Chicago Press.

Stephenson, W. (1953b). Postulates of behaviorism. *Philosophy of Science, 20*(2), 110–120. https://doi.org/10.1086/287250

Stephenson, W. (1960). Principles of selection of news pictures. *Journalism Quarterly, 37*(1), 61–68. https://doi.org/10.1177/107769906003700107

Stephenson, W. (1964). Application of Q-method to the measurement of public opinion. *The Psychological Record, 14*, 265–273. https://doi.org/10.1007/BF03395995

Stephenson, W. (1968). Perspectives in psychology: XXVI consciousness out—subjectivity in. *The Psychological Record, 18*, 499–501. https://doi.org/10.1007/BF03393799

Stephenson, W. (1970). Factors as operant subjectivity. In C. E. Lunneborg (Ed.), *Current problems and techniques in multivariate psychology: Proceedings of a conference honoring Professor Paul Horst* (pp. 33–48). University of Washington.

Stephenson, W. (1977). Factors as operant subjectivity. *Operant Subjectivity*, *1*(1), 3–16. https://ojs.library.okstate.edu/osu/index.php/osub/article/view/9351 (Original work published 1970)

Stephenson, W. (1978). Technique of factor analysis. *Operant Subjectivity*, *2*(1). https://doi.org/10.15133/j.os.1978.010

Stephenson, W. (1979). The communicability and operancy of self. *Operant Subjectivity, 3*(1), 2–14. https://doi.org/10.15133/j.os.1979.018

Stephenson, W. (1980). Factor analysis. *Operant Subjectivity, 3*(2), 38–57. https://doi.org/10.15133/j.os.1980.002

Stephenson, W. (1993). Introduction to Q Methodology. *Operant Subjectivity, 17*(1/2), 1–13. https://doi.org/10.15133/j.os.1993.006

Talbott, A. D. (2010). The Q-block method of indexing Q typologies. Presented at the AEJ Conference, Lincoln, Nebraska. Reprinted in *Operant Subjectivity, 34*(1), 6–24. https://doi.org/10.15133/j.os.2010.001 (Original work published 1963)

Thompson, G. C. (1886–1966). The evaluation of public opinion. In B. Berelson & M. Janowitz (Eds.), *Reader in public opinion and communication* (2nd ed., pp. 7–12). Free Press. Reprinted from *Public opinion and Lord Beaconsfield* (pp. 29–37), by permission of the publisher, Macmillan Co.

Thompson, J. D., Herman, G. L., Scheponik, T., Oliva, L., Sherman, A., Golaszewski, E., Phatak, D., & Patsourakos, K. (2018). Student misconceptions about cybersecurity concepts: Analysis of think-aloud interviews. *Journal of Cybersecurity Education: Research & Practice*, *2018*(1), Article 5. https://digitalcommons.kennesaw.edu/jcerp/vol2018/iss1/5

Thomson, G. H. (1935). Group factors in school subjects. *British Journal of Educational Psychology, 5*(2), 194–199. https://doi.org/10.1111/j.2044-8279.1935.tb03255.x

Turton, W., & Mehrotra, K. (2021, September 9). UN computer networks breached by hackers earlier this year. *Bloomberg.com*. https://www.bloomberg.com/news/articles/2021-09-09/united-nations-computers-breached-by-hackers-earlier-this-year?leadSource=uverify+wall

van Eeten, M. J. (2001). Recasting intractable policy issues: The wider implications of the Netherlands civil aviation controversy. *Journal of Policy Analysis & Management, 20*(3), 391–414. https://doi.org/10.1002/pam.1000 van Exel, J., de Graaf, G., & Brouwer, W. B. F. (2006). Everyone dies, so you might as well have fun! Attitudes of Dutch youths about their health lifestyle. *Social Science & Medicine, 63*(10), 2628–2639. https://doi.org/10.1016/j.socscimed.2006.06.028

van Exel, J., de Graaf, G., & Brouwer, W. (2007). Care for a break? An investigation of informal caregivers' attitudes toward respite care using Q-methodology. *Health Policy, 83*, 332–342. https://doi.org/10.1016/j.healthpol.2007.02.002

van Exel, J., de Graaf, G., & Brouwer, W. B. F. (2008). Give me a break! Informal caregiver attitudes towards respite care. *Health Policy, 88*, 73–87. https://doi.org/10.1016/j.healthpol.2008.03.001

Wacholtz, L. E. (1992a). *The communication of recorded country music: A Q-technique portrait of seven listener types* (Doctoral dissertation, The Ohio State University]

Wacholtz, L. E. (1992b, October). *The country music audience: A Q-technique portrait of seven listener types* [Paper]. International Society for the Scientific Study of Subjectivity, Columbia, MO.

Wang, Z., Sun, L., & Zhu, H. (2020). Defining social engineering in cybersecurity. *IEEE Access, 8*, 85094–85115.

Watts, S. (2011). Subjectivity as operant: A conceptual exploration and discussion. *Operant Subjectivity, 35*(1), 37–47. https://ojs.library.okstate.edu/osu/index.php/osub/article/view/8793

Watts, S., & Stenner, P. (2012). *Doing Q methodological research: Theory, method and interpretation*. Sage.

Wiederhold, B. K. (2014). The role of psychology in enhancing cybersecurity. *Cyberpsychology, Behavior, & Social Networking, 17*(3), 131–132. https://doi.org/10.1089/cyber.2014.1502

Wilson, D. D. (2006). Revealing shifts in attitude among undergraduates participating in academic service learning programs. *Operant Subjectivity*, *30*(1/2), 23–51. https://ojs.library.okstate.edu/osu/index.php/osub/article/view/8843

Wingreen, S. C., & Blanton, J. E. (2018). IT professionals' person–organization fit with IT training and development priorities. *Information Systems Journal, 28*(2), 294–317. https://doi.org/10.1111/isj.12135

Wolf, M. M. (1978). Social validity: The case for subjective measurement or how applied behavior analysis is finding its heart. *Journal of Applied Behavior Analysis, 11*, 203–214. https://doi.org/10.1901/jaba.1978.11-203

Authors and Affiliations

Rita Olla[1] · **Ramona A. Houmanfar**[1] · **Shamik Sengupta**[2] · **Emily M. Hand**[2] · **Sushil J. Louis**[2]

✉ Rita Olla
rolla@unr.edu

Ramona A. Houmanfar
ramonah@unr.edu

Shamik Sengupta
ssengupta@unr.edu

Emily M. Hand
emhand@unr.edu

Sushil J. Louis
sushil@unr.edu

[1] Department of Psychology, University of Nevada, Reno, NV, USA

[2] Department of Computer Science & Engineering, University of Nevada, Reno, NV, USA