


Development and Psychometric Analysis of Cyber Ethics Instrument (CEI)

Winfred Yaokumah, University of Ghana, Ghana

 <https://orcid.org/0000-0001-7756-1832>

ABSTRACT

This study developed and validated the psychometric properties of a new instrument, cyber ethics instrument (CEI), for assessing cyber ethics. Items related to cyber ethics were generated from a review of both scholarly and practitioner literature for the development of the instrument. The instrument was administered to university students. A sample of 503 responses was used for exploratory factor analysis (EFA) to extract the factor structure. The results of EFA suggested a six-factor structure (cyber privacy, computer ethics, academic integrity, intellectual property, netiquette, cyber safety), explaining 67.7% of the total variance. The results of confirmatory factor analysis (CFA) showed acceptable model fit indices. Therefore, the results established the viability of CEI for measuring cyber ethics. The instrument is essential for advancing the field of cyber ethics research as it will serve as a tool educators and researchers can use to measure the current stage of cyber ethics. The results obtained from using CEI can help identify and recommend cyber ethics interventions.

KEYWORDS

Academic Integrity, Computer Ethics, Cyber Ethics, Cyber Ethics Instrument, Cyber Privacy, Cyber Safety, Intellectual Property Right, Netiquette

INTRODUCTION

Developments in cyber technologies have brought about ethical issues in governmental, financial and education institutions (Pattison, 2020), and within socio-demographic groups such as the rich and the poor, gender, developed and developing nations (Tavani, 2013). Among the major concerns is the problem of cyber ethics. Cyber ethics represents ethics in the use of cyberspace (Kumar & Nanda, 2019). Cyber ethics issues are evident in areas such as cyber terrorism and warfare, cyber espionage on governments (Parasuraman & Kumar, 2020), plagiarism in education institutions (Mutula, 2011), cybercrime and cyber fraud in financial institutions, and computer misuse in organizations. Research in the recent times has been concentrating on cyber ethics, which is the “study of moral, legal, and social issues involving cyber technology” (Tavani, 2007, p. 3). Cyber technology involves “a wide range of computing and communication devices, from standalone computers to connected or networked computing and communication technologies” (Tavani, 2007, p. 3). Thus, cyber ethics seeks to examine the effect of the use of cyber technology on social, legal, and moral systems. It evaluates the social

DOI: 10.4018/IJT.2021010104

Copyright © 2021, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

policies and laws that have been framed in response to issues arising from the development and use of the laws (Ferguson et al., 2020; Tavani, 2013), while attempting to address what is right, what is just, and what is fair in the use of computers (Onyancha, 2015).

The scope of cyber ethics spans cyberspace psychology, privacy, Internet safety (Michael et al., 2019), responsible computing, cyber-harassment (Millman, Winder, & Griffiths, 2017), cyber-bullying (Stern & Felmlee, 2017), hate speech, hacking, netiquette, cyber-citizenship (Whittier, 2013), and computer ethics (Tavani, 2013). According to Chih-Ming et al. (2018), interpersonal interactions, social justice, information sharing, and self-discipline are the important virtues that foster positive behaviours in cyberspace. Ethical issues in cyberspace also include intellectual property rights, confidentiality and privacy, data security (Mutula, 2011), cyber safety (Amin, 2019), and plagiarism (Strader et al., 2014). In particular, plagiarism is a challenging problem in education institutions (Perez-Pena, 2012; Yaokumah, 2020), as high as eighty-two percent of undergraduate students were found to have been involved in plagiarism (Novotney, 2011).

With the purpose of encouraging ethical conduct (Burmeister, 2017), codes of ethics have been developed to guide appropriate behaviours of members of computing related professional bodies (Association for Computing Machinery, 2018; Computer Ethics Institute, 1992; Institute of Electrical and Electronics Engineers, 2014). Similarly, cyber laws (Copyright Act, 2005; Data Protection Commission, 2012) have been promulgated to control the conduct of people in cyberspace. Some instruments have been developed to measure computer ethics of Internet users. Among them are the Computer and Internet Activity Questionnaire (CIAQ) (Oliver, 2002), Copyright and Computer Ethics (Swain & Gilmore, 2001), a survey instrument for Information and Communication Technologies (ICT) (Jung, 2009), and Ethical Dilemmas in Computing Test (EDICT) (Bickel et al., 1992). The problem with these available codes of ethics and the computer ethics instruments is that they either do not have strong psychometric properties (Supavai, 2014), making them unreliable for measuring cyber ethics or are outmoded as a result of rapidity of technological changes (Burmeister, 2017; Kouatli, 2017).

Based on the normative ethics theory, the current study aims at developing and validating the psychometric properties of a cyber ethics scale, referred to as Cyber Ethics Instrument (CEI). Since cyber ethics scales with strong psychometric properties are sparse (Supavai, 2014), this instrument is essential for advancing the field of cyber ethics research. It will serve as a tool educators and researchers can use to measure the current stage of students' ethical judgement in cyberspace. Besides, the results of the use of CEI can help identify and recommend cyber ethics interventions. To achieve this objective, the study addresses the following questions:

1. What are the psychometric properties of the proposed Cyber Ethics Instrument (CEI)?
2. How does CEI compare with other instruments that measure similar constructs?

The rest of the study is organized as follows. The next section presents the literature review, which discusses ethics theories, empirical studies in the field of cyber ethics, and practitioner works on ethical codes of conduct. This is followed by the methodology, which explains the process of the instrument development. Next, the study presents the results and the discussion of the findings. The final section concludes with theoretical and managerial implications and future research direction.

LITERATURE REVIEW

Ethics Theories

Ethics is a branch of philosophy that deals with “values relating to human conduct, with respect to the rightness and wrongness of certain actions and to the goodness and badness of the motives and ends of such actions” (Frankena, 1963). The Encyclopaedia Britannica (2011) defines ethics as “the discipline concerned with what is morally good and bad, right and wrong” (p. 665). Ethics includes

19 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/article/development-and-psychometric-analysis-of-cyber-ethics-instrument-cei/269435

Related Content

The Case Against Weapons Research

John Forge (2014). *International Journal of Technoethics* (pp. 1-10).
www.irma-international.org/article/the-case-against-weapons-research/116716

Internet Advertising: Legal Aspects in the European Union

Radomír Jakab (2012). *Investigating Cyber Law and Cyber Ethics: Issues, Impacts and Practices* (pp. 288-310).
www.irma-international.org/chapter/internet-advertising-legal-aspects-european/59948

Anthropogenesis and Dynamics of Values Under Conditions of Information Technology Development

Liudmila V. Baeva (2012). *International Journal of Technoethics* (pp. 37-49).
www.irma-international.org/article/anthropogenesis-dynamics-values-under-conditions/69982

The Mediating Effect of Material Cultures as Human Hybridization

L. Magnani (2007). *Information Technology Ethics: Cultural Perspectives* (pp. 31-53).
www.irma-international.org/chapter/mediating-effect-material-cultures-human/23653

Property Protection and User Authentication in IP Networks Through Challenge-Response Mechanisms: Present, Past, and Future Trends

Giaime Ginesu, Mirko Luca Lobina and Daniele D. Giusto (2008). *Intellectual Property Protection for Multimedia Information Technology* (pp. 186-205).
www.irma-international.org/chapter/property-protection-user-authentication-networks/24099