A Professional Ethics Curriculum for Cyberoperations

Abstract— Ethical standards are required for any profession. In a time when cybersecurity and cyberwar are growing concerns, information and computer science (ICS) professionals must provide education and training programs that adequately equip learners for the kinds of tasks and environments they will encounter. Following a review of critical ethical issues, the current study reviews regulatory guidelines, professional codes of conduct, and ethics training programs for ICS professionals. Collectively, this suggests that education and training should focus of ethical sensemaking to facilitate the identification of the ethical affordances of novel programs and systems in ambiguous information environments. We outline a few key ethical competencies that should be developed.

Keywords—ethical decision-making, cybersecurity, cyberoperations, ethics curriculum, cyber education

I. Introduction

Ethical concerns are an integral part of the history of computing. Charles Babbage opined that the "the gradual decline of mathematical" sciences in England. [1] Many researchers, practitioners, and commentators have described the nature of general, scientific norms. [2], [3], [4], [4] These accounts range from grounding scientific norms in human values [2] to emphasizing their distinctive nature. [4] However, approaching ethics education in the sciences in such a general manner creates a problem because it ignores the realities of day-to-day practices wherein information and computing sciences (ICS) professionals need to make sense of their physical, information, and social environments.

Following Babbage, values and ethics have been a persistent, internalized feature of ICS. [5], [6], [7] Extending these skills into ethical ambiguous territories such as cyber security, aspects of information warfare, and 'cyberwar' (collectively, cyberoperations) presents an even more daunting task. The extent to which ICS professionals engaged in cyberoperations consider or have the requisite competencies and skills to address ethical issues has not been addressed. We suggest that a systematic approach in ICS education is required. [8]

Identifying the needs of a more coherent and explicit approach to address ethical issues in the ICS curriculum requires that we consider how ethical issues can be meaningfully raised in the context of training in a manner that is relevant to low-risk daily activities and sufficiently comprehensive that it can address, low-frequency, highly consequential activities. This priority has also received attention outside of ICS. In the United States, former US President noted that ideally "every student learning AI, computer science, or data science would be exposed to curriculum and discussion on related ethics and security topics."

An approach to ICS training and education requires identification of relevant issues and the processes involved in moral judgment and ethical decision-making. In this review, we first consider the features of cyberoperations ranging from cyber security issues to cyberwarfare including the roles and responsibilities of ICS professionals engaged in those activities. We then review evidence on features of ethical education and training programs that have proven effective [inside and] outside of software engineering and provide recommendations. Finally, we consider the feature of moral development and ethical decision-making and outline an ethical sensemaking approach to ethics training and education.

II. Ethical Issues in Cyberoperations

A. Emergent Issues in Human-Technology Interfaces

We live in a highly connected, interdependent world. For this reason, cyberoperations represent the forefront of ethical issue of our time. Numerous ethical concerns are evidenced in software development and cyberoperations (e.g., [9], [10]). Illustrating this, at the physical- and information-levels, computing systems reflect dual-use technologies: they have been developed for civilian activities but can also have military applications. Consequently, software developers need to engage in vulnerability assessment and penetration testing as users will be likely unaware of these affordances of the technology that they use.

Privacy is yet another concern that affects both users and developers. Whereas users might have the expectation that their behavior is anonymous and confidential in the absence of a clear understanding of the terms and conditions of the use of an application, developers might see it as their place to be responsible for ensure privacy within an application. Moreover, secondary use of data reflects a similar concern wherein information obtained under one set of conditions might be used to inform another problem (e.g., patient records, browsing behavior). These concerns have made privacy engineering [6] and micro-targeting based on acquired data [11] topics of considerable importance. Privacy concerns are especially important with many revenue models for applications based on targeted ads. [12]

The operations and output of autonomous and intelligent systems has also become a growing concern with the observation of race- and gender-based biases. [13] Much of this concern can be attributed to the lack of transparency in deep learning algorithms as well as the data sets used to train these systems. [14] While providing new data sets might reflect a

partial solution, [15] understanding the underlying basis for the bias requires an understanding of relevant socio-cultural norms and conventions. [16], [17], [18]

A final issue concerns educational practices referred to as 'ethical hacking'. [19] Instruction in ethical hacking has become widely available. [20], [21] Ostensibly, instruction provides learners with the ability to engage in "white hat" or "grey hat" operations – penetrating a network in order to identify its vulnerabilities. By providing these lessons, educators have given learners the tools to engage in malicious activities. [22] In the absence of monitoring and regulation mechanisms, educators are leaving ICS professionals to make decisions on their own.

B. Responsibilities of Developers.

Developers and network security professionals must be located at the core of ethics curriculum for cyberoperations. The roles and responsibilities of developers, their values and behavior, as well as the physical and virtual work environments that they operation within must be addressed in substantive ways. The requirement of continuing professional development (CPD) [23], [24] should also be a feature of an ethics curriculum.

In most cases, developers will need to consider how a user will typically interact with the networks, software, and interpret the output of these systems. A number of ethical issues have been identified in the academic and grey literatures [25]. These issues include how to treat log files containing user activities, the level of encryption required, whether and to what extent a program, anticipating how software can be misused, and how much effort should be placed in defending users' data if it is requested by a governmental organization. In most cases, responses to each of these questions is nuanced and will require a consideration of an organizations code of conduct, collective agreements, licencing agreements, as well as local, national laws, and international laws.

In the context of cyberoperations associated with conflict, there will likely be significant conflict of values and competencies between respect for privacy and sovereignty in the process of ethical hacking. When a software engineer is being trained, they are unlikely to consider themselves as 'combatants' in a 'war' between nations. Moreover, as Beard (2016) notes, "not all cyberoperatives [will] fight war" (p. 148). However, at present and for the foreseeable future, they are more likely to be find themselves directly or indirectly involved in cyberoperations such as defending critical infrastructure against cyberattacks. How they understand, and are trained to understand, these activities cannot be ignored. For instance, while a cyberoperation might have intended consequences (e.g., to disable a network or infrastructure), it can also have unintended consequences to adjacent systems. By highlighting the wider implication of using these tools, ICS professions can become more effective judges of their own actions and should consider the inclusion of features that eliminate unnecessary intrusions or disruptions in unrelated networks.

C. Responsibilities to Users

ICS professionals are not the only individuals who have responsibilities. Users have an important role in terms of how they use and maintain their devices. Collectively, these can be referred to as cyber hygiene practices which include updating software, running malware scans, and adopting appropriate security protocols for password protection. While developers are not educators or monitors of these behaviours, they must consider how to promote cyber hygiene practices in the development and use of their software. User are especially unlikely to see themselves as an attack vector in a cyberoperation. For instance, a mobile phone has an intended use (e.g., texting, checking email, making phone calls, taking photos) while it can also be used as an attack surface (e.g., as a node in a botnet engaging in a DDoS). Moreover, evidence suggest that users do not understand the nature of targeted advertising suggesting that wider efforts are required to educate users. [26]

The IEEE has also emphasized this priority, noting that "[Autonomous and Intelligent Systems] creators shall empower individuals with the ability to access and securely share their data, to maintain people's capacity to have control over their identity." [9] This will reflect a process of knowledge translation whereby developers render intelligible the benefits of practices such as updating software, running malware scans, and selecting sufficiently complex passwords. More generally, developers must be better trained to translate their knowledge of vulnerabilities in a manner that is intelligible to users, a question that parallels the notion of explainable AI (XAI). For instance, ACM (2007) highlights the need for transparency and accountability in the development of algorithms supported by concerns over potential bias in algorithms. [14]

III. Ethics in Information Science

Systematic reviews and implementation of comprehensive ethics education and training program has not yet been undertaken (cf. reviews of ethical AI [27], [28]). However, a number of sources can inform curriculum development including general frameworks and guidelines, codes of conduct provided by professional societies, and finally research on ethics and training programs in the ICS professions.

A. General Frameworks and Guidelines

There is a growing trend to develop guidelines to address ethical issues in ICS. In Europe, the European Commission has developed a framework. The General Data Protection Regulations (GDPR) emphasize clarity of language provided to the user, affirmative consent from users, as well as greater accessibility and the availability of option (e.g., movement of data and the "right to be forgotten").

Similar efforts have been undertaken in the UK in terms of the *UK Data Ethics framework*. The *Framework* defines responsibilities for developers such that a user's needs are identified, minimal data is used, and data scientists must acknowledge the data used and the limits of their skillset. With the growing recognition that ethical issues are inherent in software development, these guidelines are likely to multiple. Being aware of these standards and being sufficiently competent to recognize issues in their application must be a feature of an ethics curriculum in academic institutions and with organizations employing ICS professionals.

B. Professional Codes of Conduct

Professional societies provide another source of ethical norms. Codes of conduct can be used simply as inspirational value statements, as a tool for communication, or to establish standards for monitoring and regulation of behavior within a profession. Regardless of their function, only a few standards are generally available for ICS professionals. For instance, the *IEEE Code of Conduct* [29] and the *IEEE Code of Ethics*. [30] However, norms are provided in a general form. For instance, the Code of Conduct states that all members of IEEE must "…avoid injuring others, their property, data, reputation, or employment by false or malicious action" and that they will "[c]omply with applicable laws in all countries where IEEE does business and with the IEEE policies and procedure."

Similarly, the IEEE has also developed *Ethically Aligned Design* [9] to provide which contains "high-level ethical principles" for autonomous and intelligent systems. Conforming to the *Code of Conduct* and *Code of Ethics*, these 8 principles were developed to ensure human values and trustworthiness consisting of human rights, well-being, data agency, effectiveness, transparency, accountability, misuse, and competence.

In contrast to the IEEE *Code*, the Association for Computing Machinery (ACM) recently updated its ethical standards, *ACM Code of Ethics and Professional Conduct*. [29] Likely due to the more specific area of their practitioners, more specific ethical concerns relevant to software engineering are integrated into the code. For instance, it includes reference to "[e]fforts to help others by contributing time and energy to projects that help society illustrate a positive aspect of this principle. Such efforts include free and open source software and work put into the public domain." It also considers "the inevitability of software errors, the interactions of systems and their contexts" and the impact of software updates on user productivity and work quality given user dependency (3.6).

Most notably, the *Code* also makes reference to cyberoperations. Namely, it specifies that:

> "…computing professionals should not access another's computer system, software, or data without a reasonable belief that such an action would be authorized or a compelling belief that it is consistent with the public good. A system being publicly accessible is not sufficient grounds on its own to imply authorization. Under exceptional circumstances a computing professional may use unauthorized access to disrupt or inhibit the functioning of malicious systems; extraordinary precautions must be taken in these instances to avoid harm to others."

When taken together, the ACM and IEEE codes raises concerns over a number of ethical affordances inherent in software engineering which need to be incorporated in the curriculum. Specifically, understanding what is meant by the 'public good' and who represents a legitimate authority that could authorize the violations of privacy. Yet, there are many areas wherein conflicts can arise. Namely, while the emphasis on harm avoidance is important condition, the earlier recognition that errors are inevitable requires further elaboration as to which the nature and extent to acceptable errors might be. Similarly, for those engaged in cyberoperations, these demands are likely unrealistic, instead requiring novel, concrete boundaries of conduct in these special circumstances. [10]

C. Efficacy of Ethics Training Programs

Ethics codes can provide a baseline of knowledge. Alone, they are inadequate in addressing specific concerns that ICS Professionals will encounter. Education and training programs require a consideration of their objectives and design [30] including how they use social interaction to highlight critical features of a learner's situation and how they fit into a curriculum. [31] If the educational objectives is to develop a moral sensemaking competencies in learners, methods must be identified that allow us to do this effectively. Ethics training can be a requirement of the receipt of funds (e.g., NIH; [32]). A number of approaches have emphasized critical thinking and decision-making in general [33], [34] identifying ethical sensitive features of a situation [35], [36], [37] providing developmentally appropriate training [38], [39] or advancing moral reasoning abilities. [40], [41] However theoretically reasonably these approaches might seem, a deeper question concerns their relative efficacy. For instance, the values expressed in the IEEE and ACM codes likely are in opposition to such cyberoperations framed as "ethical hacking".

Efficacy of education and training programs has been a persistent concern due to observations that performance in these tasks often are not reflected in behavior. An important illustration of the issues faced by software developers is the goal of embedding privacy preserving mechanisms in their software.

In a survey conducted by Senarath and Arachchilage [42] ICS professionals' awareness of a number of ethical issues was assessed. For instance, a larger number of developers (38.8%) identified assurance that they had implemented privacy standards as an issue, implementing privacy standards (33.3%), and a belief in the inherent contradiction of including privacy in software (27.6%). Moreover, few developers had any knowledge of basic privacy concepts. Many developers they had never heard of privacy impact assessment (47.2%), fair information practices (38.9%), privacy by design (36.1%), and data minimization (22.2%). Crucially, the majority of developers did not see privacy as a functional requirement (83.3%), suggesting that it is not deemed to be an important feature of design. [45] In another study by Balebako et al (2017), they found that many developers were often not aware of what information was collected by third-party ads (22.0%). They additional found that privacy concerns were less prevalent in samples of employees from smaller companies.

Similarly, Senarath et al. [43] examined the extent to which software developers used Privacy Engineering Methodologies (PEM, methods for including ensuring user privacy during software development). They found that the perceived usefulness of the PEM as well as their compatibility with a developer's approach were the main determinants of whether the PEM were used or not.

IV. Ethical Sesnemaking Processes

The constantly changing of information technologies and ambiguous nature of information environments means that codes of conduct will not be adequate. Instead, ICS professionals must develop judgment, reasoning, and decision-making competencies that allow them to identify the ethical affordances of the software and systems that they design and interact with.

A. Developmental Course of Moral Judgments

Moral competencies develop over time. [44], [45] Moral developmental models assume that learners pass through successive stages, with progression from preconventional reasoning (i.e., norms revolve around punishment and reward), to conventional reasoning (i.e., individuals are concerned with immediate group behavior or that of society), and, ideally, to postconventional reasoning (i.e., pragmatic rules for maximizing good and minimizing harm, or inviolable principles). Educators should then consider the development stage of a learner. In the context of ICS professionals, this will also require a consideration their understanding of information science and technology. Thus, education and training in ethical issues will likely occur after foundational knowledge and skills are developed.

B. Contexts of Moral Judgments

If moral competency develops over time and there are early biases for conformity, why are so many failures of moral judgment observed? Context has proven to be an integral feature of ethical decision-making. Thus, in addition to individual factors such as reasoning and decision-making ability, situational and organizational factors must also be taken into consideration. [46], [47], [48] On such an account, lapses in moral judgment are not simply attributable to lacking specific ethical knowledge or reasoning ability, rather, they can arise due to a failure to recognize the ethical affordances of a situation, dissimilar norms and conventions, situational stressors, and failures of self-monitoring.

Humans are sensitive to the demands of the context and their role within the situation. For instance, attitudes and behaviors frequently differ [49] and people will frequently conform to erroneous responses while maintaining an accurate understanding of the situation. [50] As Mazar et al. [51] have demonstrated, participants tend to deviate in minor ways from social norms (i.e., minor forms of cheating) unless they are provided with reminders about what conduct is typical in a situation. These results are also support in classic studies wherein participants fail to assist others when they have limited time, even when they have just completed a task that primes ethical thinking. [52] Thus, ethics training for ICS professionals must ensure that learners not only understand effective principles but the circumstances in which they might fail to a apply them. In the context of cyberoperations, ICS professionals will face potentially deep moral conflicts wherein their ethical sensemaking abilities will be stretched to their limits. Thus, advanced training is vital to prepare them for the possible situations they will encounter.

C. Moral Pluarlism

Rather than a single set of norms and conventions, ICS professionals will be confronted with moral pluralism, wherein multiple ethical frameworks are viable. Instead of assuming that these values are incommensurable and mutually unintelligible, behavioral and social science research suggest that a number of normative systems can be identified. [53] Within any situation, a number of social norms can be used to define what reflects correct and incorrect behavior. This can be understood in terms of schemata and scripts – typically, a rich set of interrelated beliefs, values, roles, and actions that an individual has learned through a process of socialization.

Cross-cultural studies suggest that multiple exchange schemata can be identified. For instance, A.P. Fiske [54] has identified multiple relational models to determine the perception of fair interactions with others that vary from perceptions of equivalence, equality, or asymmetries between group members. However, it is unclear that ICS professionals have such an understanding of multiple relational theories. For instance, cybersecurity is frequently framed in terms of the Prisoner's Dilemma wherein the outcomes of two agents' are placed in opposition to one another. [55] This fails to consider that studies using Prisoner's Dilemma frequently observation violation of equilibria associated with competition. Actual levels of cooperation in online communities must be understood in order to effectively develop software and systems for potential vulnerabilities. Ethics training needs to provide ICS professionals with a more contemporary review of psychological motivations associated with exchanges.

V. Recommendations for the Future of Ethics Education in the ICS Professions

ICS professionals can expect to encounter a number of ethical issues throughout the course of their work. Those that go into cyberoperations such as cybersecurity and cyber warfare need to be prepared for the challenges that continuously evolving software and systems that they will encounter.

Ethics curriculum need to take into consider the roles and responsibilities of ICS professionals, the ethical issues they will encounter, as well as existing professional standards. While codes of conduct and guidance documents exist [9], [29] they are not meant to be exhaustive nor can they address also aspects of a ICS professional's work. Moreover, ICS professionals will continue to work in inherently ambiguous information environments with competing ethical norms and evolving technologies.

Training and education require the development of ethical sensemaking abilities that permit the identification of the moral affordances of the situation. In that ICS professionals must see the relevance of these practices to their day-to-day operations, they should be embedded in the curriculum. While a specific course should be developed to presented to learners, there will also need to be integration. Thus, a straightforward approach is to provide learners with an initial course following the successful completion of foundational courses and then

integrate questions concerning ethical design and operations thereafter.

REFERENCES

[1] C. Babbage, Reflections on the decline of science in England, and on some of its causes., London: Kessinger Publishing Company, 1830/2004.

[2] J. Bronowski, Science and Human Values, New York: Harper Torchbooks, 1965.

[3] R. K. Merton, "The Normative Structure of Science.," in *Storer, N.W. (1973) The Sociology of Science*, Chicago, University of Chicago Press, 1942, pp. 267-278.

[4] J. Ziman, Real Science: What it is and What it Means, Cambridge, 2000.

[5] P. Himanen, L. T and M. C, The Hacker Ethic, New York: Random House, 2001.

[6] S. Gürses and J. M. del Alamo, "Privacy Engineering: Shaping an Emerging Field of Research and Practice," *IEEE Security & Privacy,* vol. 14, 2016.

[7] R. Boyle and M. Clark, "CS++ content is not enough," *ACM SIGCSE Bulletin,* vol. 36, pp. 422-426, 2004.

[8] T. Wulf, "Teaching ethics in undergraduate network," *Consortium for Computing Sciences in College,* vol. 19, 2003.

[9] I. G. Initiative, Ethically aligned design, Version 1, IEEE Standards, 2016.

[10] F. Allhoff, A. Henschke and B. J. Strawser, Binary bullets: The Ethics of Cyberwarfare, Oxford University Press, 2016.

[11] G. R. Murray and A. Scime, "Microtargeting and electorate segmentation: data mining the American National Election Studies," *Journal of Political Marketing,* vol. 9, pp. 143-166, 2010.

[12] T. Book, A. Pridgen and D. S. Wallach, "Longitudinal Analysis of Android Ad Library Permissions," *Proceedings of MoST 2013,* 2013.

[13] H. Devlin, "Discrimination by Algorithm: Scientists Devise Test to Detect AI Bias," *The Guardian,* 18 Dec 2016.

[14] R. Thomson, E. Alhajjar, I. J and T. Russell, "Predicting bias in machine learned classifiers using clustering," in *Annual Social Computing, Behavior Prediction, and Modeling-Behavioral Representation in Modeling Simulation Conference 2018.*, 2018.

[15] M. Hardt, E. Prince and N. Srebro, "Equality of Opportunity in Supervised Learning," in *Proceedings of the 30th International Conference on Neural Information Processing Systems*, Barecelona, Curran Assocaites Inc., 2016, pp. 3323-3331.

[16] N. Garg, L. Schiebinger, D. Jurafsky and J. Zou, "Word embeddings quantify 100 years of gender and ethnic stereotypes," *Proceedings of the National Academy of Sciences,* vol. 115, pp. E3635-44, 2018.

[17] A. Caliskan, J. J. Bryson and A. Narayanan, "Semantics derived automatically from language corpora contain human-like biases," *Science,* vol. 356, pp. 183-186, 2017.

[18] J. Zhao, T. Wang, M. Yatskar, V. Ordonez and K. W. Chang, "Men also like shopping: Reducing gender bias amplification using corpus-level constraints," *arXiv preprint arXiv:1707.09457 ,* 2017.

[19] C. C. Palmer, "Ethical hacking," *IBM Systems Journal,* vol. 40, pp. 769-780, 2001.

[20] A. Harper, S. Harris, J. Ness, C. Eagle, G. Lenkey and T. Williams, Gray Hat Hacking: the Ethical Hackers Handbook, McGraw-Hill Osborne Media, 2011.

[21] P. Engebretson, The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy, Elsevier., 2013.

[22] D. Jamil and M. N. Khan, " Is ethical hacking ethical.," *International journal of Engineering Science and Technology,* vol. 3, pp. 3758-3763, 2011.

[23] A. Kennedy, "Models of continuing professional development: A framework for analysis," *Journal of In-Service Education,* pp. 235-250., 2005.

[24] C. Peck, M. McCall, B. McLaren and T. Rotem, "Continuing medical education and continuing professional development: international comparisons," *British Medical Journal,* vol. 320, pp. 432-435, 2000.

[25] P. Wayner, "12 Ethical Dilemmas Gnawing at Developers Today," *InfoWorld,* pp. Retrived from: https://www.infoworld.com/article/2607452/12-ethical-dilemmas-gnawing-at-developers-today.html, 12 April 2014.

[26] B. Ur, P. G. Leon, L. F. Cranor, R. Shay and Y. Wang, "Smart, useful, scary, creepy: perceptions of online behavioral advertising," in *Proceedings of the Eighth Symposium on Usable Privacy and Security*, 2012, pp. 1-15.

[27] A. Jobin, M. Ienca and E. Vayena, Artificial Intelligence: the global landscape of ethics guidelines, arXiv preprint arXiv:1906.11668. , 2019.

[28] J. Fjeld, N. Achten, H. Hilligoss, A. Nagy and M. Srikumar, Principled Artificial Intelligence: Mapping Consensus in Ethical and Rights-based Approaches to Principles for AI, Berkman Klein Center Research Publication, 2020.

[29] A. Council, ACM Code of Ethics and Professional Conduct, https://ethics.acm.org/code-of-ethics/: ACM, 2018.

[30] S. I. Tannenbaum and Y. G, " Training and development in work organizations," *Annual review of psychology,* vol. 43, pp. 399-441, 1992.

[31] J. R. Schoenherr and S. J. Hamstra, "Beyond fidelity: deconstructing the seductive simplicity of fidelity in

simulator-based education in the health care professions," *Simulation in Healthcare,* vol. 12, pp. 117-123, 2017.

[32] R. Dalton, "NIH cash tied to compulsory training in good behaviour.," *Nature,* vol. 408, p. 629, 2000.

[33] N. C. Frisch, "Value analysis: A method for teaching nursing ethics and promoting the moral development of students," *Journal of Nursing Education,* vol. 26, pp. 328-332, 1987.

[34] A. L. Gaul, "The effect of a course in nursing ethics on the relationship between ethical choice and ethical action in baccalaureate nursing students," *Journal of Nursing Education,* vol. 26, pp. 113-117, 1987.

[35] H. Clarkeburn, "A test for ethical sensitivity in science," *Journal of Moral Education,* vol. 31, pp. 439-453, 2002.

[36] H. Clarkeburn, D. J. R and B. Matthew, "Impact of an ethics programme in a life sciences curriculum," *Teaching in Higher Education,* vol. 7, pp. 65-79, 2002.

[37] L. Myyry and K. Helkama, "The role of value priorities and professional ethics training in moral sensitivity," *Journal of Moral Education,* vol. 31, pp. 35-50, 2002.

[38] M. J. Bebeau and S. J. Thoma, "The impact of a dental ethics curriculum on moral reasoning," *Journal of Dental Education,* vol. 58, p. 684, 1994.

[39] L. Duckett, M. Rowan, M. Ryden, K. Krichbaum, M. Miller, H. Wainwright and K. Savik, "Progress in the moral reasoning of baccalaureate nursing students between program entry and exit," *Nursing Research,* vol. 46, pp. 222-229, 1997.

[40] S. A. Goldman and J. Arbuthnot, "Teaching medical ethics: the cognitive-developmental approach," *Journal of Medical Ethics,* vol. 5, p. 170, 1979.

[41] W. Y. Penn, "Teaching ethics-a direct approach," *Journal of Moral Education,* vol. 19, pp. 124-138, 1990.

[42] A. Senarath and N. A. Arachchilage, "Why developers cannot embed privacy into software systems? An empirical investigation," in *Proceedings of the 22nd International Conference on Evaluation and Assessment in Software Engineering* , 2018, pp. 211-216.

[43] A. Senarath, M. Grobler and N. A. Arachchilage, "Will they use it or not? Investigating software developers' intention to follow privacy engineering methodologies.," *ACM Transactions on Privacy and Security (TOPS),* vol. 22, pp. 1-30, 2019 .

[44] J. Piaget, The Moral Judgment of Children, London: Routledge & Kegan-Paul, 1932.

[45] L. Kohlberg, "Moral stages and moralization: the cognitive-developmental approach," in *T. Lickona (Ed.), Moral Development and Behavior: Theory, Research and Social Issues*, New York, Holt, Rinehart and Winston, 1976, pp. 31-54.

[46] A. L. Antes, R. P. Brown, S. T. Murphy, E. P. Waples, M. D. Mumford, C. S and D. L. D, "Personality and ethical decision-making in research: The role of perceptions of self and others," *Journal of Empirical Research on Human Reesearch Ethics,* vol. 2, pp. 15-34, 2007.

[47] L. K. Treviño, "Ethical decision making in organizations: A person-situation interactionist model," *The Academy of Management Review,* vol. 11, pp. 601-617, 1986.

[48] L. K. Treviño, G. R. Weaver and S. J. Reynolds, " Behavioral ethics in organizations: A review," *Journal of Management,* vol. 32, pp. 951-990, 2006.

[49] L. R. Glasman and D. Albarracin, "Forming attitudes that predict future behavior: A meta-analysis of the attitude-behavior relation.," *Psychological bulletin,* vol. 778, p. 778, 2006.

[50] R. Bond and P. B. Smith, "Culture and conformity: A meta-analysis of studies using Asch's (1952b, 1956) line judgment task," *Psychological bulletin,* vol. 119, p. 111, 1996 .

[51] N. Mazar, O. Amir and D. Ariely, "The dishonesty of honest people: A theory of self-concept maintenance.," *Journal of marketing research. ,* vol. 45, pp. 633-644, 2008.

[52] J. M. Darley and C. D. Batson, "From Jerusalem to Jericho": A study of situational and dispositional variables in helping behavior," *Journal of Personality and Social Psychology,* vol. 27, p. 100., 1973.

[53] J. Graham, J. Haidt, S. Koleva, l. M. Moty, R. Iyer, S. P. Wojcik and P. H. Ditto, "Moral foundations theory: The pragmatic validity of moral pluralism," in *Advances in Experimental Social Psychology*, Academic Press, 2013, pp. 55-130.

[54] A. P. Fiske, Structures of Social Life: The Four Elementary Forms of Human Relations, Free Press, 1991.

[55] C. T. Do, N. H. Tran, C. Hong, C. A. Kamhoua, K. A. Kwiat, E. Blasch, S. Ren, N. Pissinou and S. S. Iyengar, "Game theory for cyber security and privacy," *ACM Computing Surveys (CSUR),* vol. 50, pp. 1-37, 2017.

[56] M. Weber, "Science as Vocation," in *From Max Weber: Essays in Sociology. Translated, ed.*, New York, Oxford University Press, 1946.

[57] L. Myyry and K. Helkama, "The role of value priorities and professional ethics training in moral sensitivity.".

[58] I. I. Mitroff, The Subjective Side of Science: A Philosophical Inquiry into the Psychology of the Apollo Moon Scientists, Amsterdam: Elsevier, 1974.