NetDefense: A Tower Defense Cybersecurity Game for Middle and High School Students

William Toledo
College of Education
University of Nevada, Reno
Reno, Nevada, USA
wtoldeo@unr.edu

Sushil J Louis
Department of Computer Science
University of Nevada, Reno
Reno, Nevada, USA
sushil@unr.edu

Shamik Sengupta
Department of Computer Science
University of Nevada, Reno
Reno, Nevada, USA
ssengupta@unr.edu

***Abstract*—This Innovate Practice Full Paper presents a new game for cybersecurity learning. Cybersecurity education is critical to personal media consumption, privacy protection, and national infrastructure. We live in a world that is increasingly connected; the majority of people, particularly young people, engage with technology and social media for multiple hours per day, using the internet as a source of news, entertainment, and connection to the outside world. However, threats on the internet, including misinformation, disinformation, phishing, and multiple other cybersecurity threats grow each year. Because of this, cybersecurity is an essential skill for K-12 and all undergraduate students to learn in public schools. In this study, we asked K-12 teachers to analyze a specific game, NetDefense, designed to teach students basic cybersecurity concepts related to networking. NetDefense specifically addresses concepts within the network communications component of the core theme of computing systems from the K-12 cybersecurity standards released by cyber.org. Before and after engaging with the game, we asked teachers a series of survey questions to determine their perceptions of the game and its utility in classrooms. Findings indicate that NetDefense improved teachers' knowledge of network concepts. Participating teachers believed that NetDefense would help students learn these concepts and that NetDefense is an appropriate tool for this type of learning. Finally, teachers believed that student motivation to learn about and use cybersecurity concepts would increase upon playing the game. We plan to improve the game using feedback from our participants, disseminate the open source, publicly available game to all interested educators for classroom and laboratory use, and gather more data on game effectiveness.**

***Index Terms*—Cybersecurity, Computer game, K-12 Teachers, Survey**

I. Introduction

We live in a world that is increasingly connected; the majority of people, particularly young people, engage with technology and social media for multiple hours per day, using the internet as a source of news, entertainment, and connection to the outside world [1]. However, the threats on the internet, including misinformation, disinformation, phishing, and multiple security threats grow each year. Because of this, media literacy is an essential skill for pre-K-12 students to learn in public schools [2]. A key, and often overlooked, aspect of media literacy is cybersecurity, or the skills and dispositions needed to protect one's privacy, identity, and personal information online. In this study, we asked pre-K-12 teachers to analyze a specific game, NetDefense, designed to teach students basic cybersecurity concepts related to networking. NetDefense specifically addresses concepts within the network communications component of the core theme of computing systems from the K-12 cybersecurity standards released by cyber.org. Before and after engaging with the game, we asked teachers a series of survey questions to determine their perceptions of the game and its utility in classrooms. NSA, NSF, and other agencies involved in workforce development are funding programs that teach cybersecurity concepts early (K-12) and help inform and motivate such students into pursuing cybersecurity careers. Specifically, we have a Research Experience for Teachers (RET) from the NSF and teachers in our program from middle and high schools spend six weeks in the summer participating in research experiences and developing classroom modules and materials which are implemented in their classrooms during subsequent academic years. These projects involve partnerships between the university, the school districts in surrounding counties, and local industry. The project develops and fosters a community of teachers who are passionate about cybersecurity and who can translate this excitement to their students through engaging, high-quality inquiry learning experiences. We thus had the opportunity to work with practicing teachers to examine their perception and knowledge related to cybersecurity, and specifically the relationship between cybersecurity and the ability to teach related concepts and content through a virtual game platform. In the next section, we outline the importance of cybersecurity in global economies and societies, and the importance of educating students and the public on key concepts

This work was supported by grant number N00014-22-1-2122 from the Office of Naval Research. The views, opinions, findings and conclusions reflected in this publication are solely those of the authors and do not represent the official policy or position of our sponsors.

II. Prior work

Over the past several years, we have seen significant progress in advancing Cyberspace and Cyber-Physical systems technology. The evolution of smart grids, IoT, connected vehicles, biometric devices, and social networks are all part of this increasingly complex cyberspace. Growing dependency on this cyberspace also means that new threats will be emerging that must be addressed in order to keep our infrastructure

resilient. Defense from modern day attackers such as hackers, terrorists, skilled corporate raiders and vandals has become a critical issue for all cyber-consumers. Cyber-crime costs the global economy over US $400 billion per year, and is projected to reach $2 Trillion by 2019 [3]. For example, cyber-attacks on Home Depot [4] lasted five months, and breached 56 million customers' credit and debit card information. Such cyberwar has expanded to the health-care, energy, and financial sectors as well. Multiple data breaches on one of the nation's largest banks, JP Morgan Chase [5], affected millions of households and businesses, while data breaches at Anthem and Primera Blue exposed nearly 90 million consumers' health insurance/health records [6]. A cyber-attack on Experian credit services, affected approximately 15 million customers [7], and recently, a cybergang successfully infiltrated more than 30 global financial institutions' payment systems using sophisticated malware named "carbanak" [8]. We are also seeing evolving exploits such as "Industroyer" or "Crash Override" which are starting to target critical cyber-physical infrastructure and power grids [9].

With rapidly changing computing and cyber-physical systems, new attack patterns are always evolving [10]–[12]. We thus cannot overstate the need and significance of cybersecurity education in the context of STEM Education. The National Science and Technology Council (NSTC) also issued a coordinated Federal strategic plan for cybersecurity research and education: "As a foundation that enables safety and innovation in cyberspace, cybersecurity is of fundamental importance to the economic strength and national security of the United States ... cybersecurity has not kept pace with the increase in cyber threats. Advances in cybersecurity science and engineering are urgently needed to ... establish position of assurance, strength, and trust for cyber systems and professionals" [13].

To advance this goal, we developed NetDefense: a cybersecurity game (i) to explore unique ways to engage Middle and High School (Ms/Hs) teachers and students in cybersecurity and (ii) to create a fun-filled interactive environment for students to learn basic concepts of cybersecurity from an early age. In the next section the NetDefense platform, its design, and how it helps advance the goals of increasing public knowledge of key concepts in K-12 school sites.

III. NetDefense

Games provide several nice properties. They can capture a player's imagination with engaging visualizations and appealing back-story lines. Being interactive, they can educate in engaging participatory ways. Students can play individually and in groups and have "fun" laboratory work helping leverage teacher's time and reach. Gamification, the application of typical elements of game playing to other areas of activity (such as education) to encourage engagement with a product or service, has grown to encompass areas as diverse as marketing and healthcare and shown significant positive impacts in fostering engagement and retaining knowledge and skills [14].

We thus developed the NetDefense game to help teach low-level computer networking concepts related to cybersecurity to middle and high school students. NetDefense is designed to teach the concept of discrete data packets, good/bad packets, filtering using firewalls, firewall placement, firewall filter design and network log analysis to understand the anatomy of simple cybersecurity defense design. Figure 1 shows screenshots from NetDefense The screenshots show

Fig. 1. Screenshots from NetDefense showing different skins for different sectors of the economy.

multiple "skins," or game graphic asset swaps, corresponding to different sectors of the economy that may be affected by cybersecurity breaches.

We chose to use the popular *Tower Defense* genre of video games upon which to model cybersecurity defense. Netdefense is therefore a tower defense game and has similar game mechanics and gameplay. Tower defense games feature defense of structures by emplacing defensive fortifications along possible attack paths. Mapping servers to structures that need defending, routers to defensive fortifications, and firewall rules to rules for automated defensive engagements, NetDefense elegantly maps network cybersecurity concepts to tower defense. Furthermore, we can easily swap game "skins" to communicate that cybersecurity affects different industries using different skins.

As in most tower defense games, packets both good and malicious move from sources to servers. Players need to identify malicious packets sent by a "blackhat" and place and configure routers to filter out (destroy) such packets. Router placement is important in cybersecurity defense. Consequently, judicious router placement was incorporated in gameplay by enabling router placement along paths and limiting the number of available routers. Incorrect router placement would lead to lower scores since some data packets would be able to take paths without a router on that particular path to a server. Correct router configuration, that is, correctly specifying the shape, color, and size of packets to be filtered, increased the game score which was computed as the fraction of malicious packets filtered.

Figure 2 shows screenshots from a more recent version of the game modeled on the populat "Tron" movie and its recent reboot. On the left is the "Whitehat"'s or defensive player's screen. The black cubes represent network packet sources (red) and sinks or servers that must be defended (blue). Data communication packets follow available paths from sources to servers. As the whitehat player, your job is to place routers along paths and specify router rules that filter out malicious packets to maximize your score. The center screenshot shows the new window (lower left) to specify simple filtering rules and the router for which we are specifying the rules. The

simple rules with packet shape, color, and size and can be quickly understood and specified by all levels of players. The selected router (the router for which we are specifying rules) is denoted by the green selection circle. The rightmost screenshot shows the score at the end of a game phase and some statistics on the data packets. The game has three levels of difficulty: easy, medium, and hard. Honeypots to draw away malicious packets only appear at the hard level. In the medium level, packets move faster and it is more difficult to differentiate malicious and non-malicious packets. In the easy level of the game, malicious packets have a red circle to be easily identifiable.

Fig. 2. Screenshots from the current "Tron" version of NetDefense

The opponent ("Blackhat") player specifies the relative proportion of malicious packets sent to each blue server and the properties (shape, color, size) of the malicious packet. The current single player version of this game has a simple Blackhat AI that randomly picks proportions and properties and a simple Whitehat AI that uses a gradient ascent algorithm to induce filtering rules from malicious packets' effects.

The game was written from scratch in Unity3d and can be easily exported as a WebGL game hosted on a web server. This enables easy player access to the game. We designed NetDefense to store information about player decisions, timing, and scores on the web server backend so that, in the future, we may add leaderboards and other gamification structures to help popularize the game. In addition, we may also use anonymized collected data for measuring game effectiveness in imparting cybersecurity knowledge. Current and past RET teacher cohorts will help disseminate the game to our target population this fall.

IV. Methodology

We evaluate NetDefense's utility by asking K-12 teachers to play the game and surveying their responses to a series of survey questions to determine their perception of the game and its utility in classrooms or laboratories. The work described uses the Tron version of NetDefense.

Specifically, we gathered and analyzed data from cybersecurity and computer science K-12 teachers in order to improve the game and to obtain feedback on potential effectiveness and motivational impetus. We used Google forms to implement pre-game and post-game surveys to obtain teacher opinions and suggestions on the game. In this paper, we examine trends in our data using qualitative [15] and quantitative [16] data analysis methods related to (a) teachers' perceived levels of knowledge related to cybersecurity, (b) teachers' perceptions of game-based learning related to cybersecurity, and (c) teachers' perceptions of student learning outcomes.

V. Results and Findings

A. Teacher Levels of Knowledge

We examined teachers' perceived levels of knowledge of different key concepts in our pre- and post-surveys. Participants rated their perceived current levels of knowledge on four concepts: (a) packets, (b) packet filtering, (c) firewalls, and (d) honeypot. The most common responses across all four concepts were "fair" and "satisfactory." The only concept that participants ranked their knowledge as "excellent" was packets, which had two participants rank their level of knowledge as excellent. Figure 3 displays teachers' pre-survey perceptions

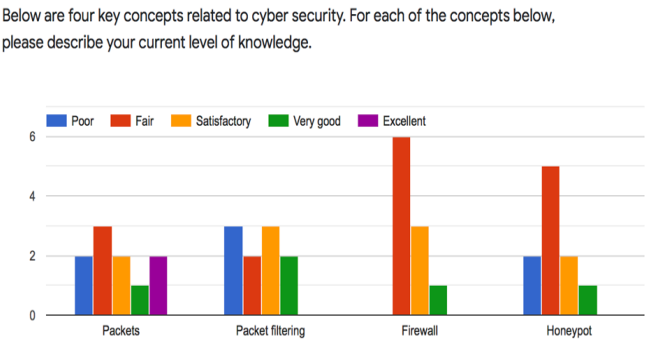

Fig. 3. Pre-exposure survey: Teachers' Perceived Levels of Knowledge.

of their own cybersecurity knowledge, and Figure 4 displays teachers' post-survey perceptions.

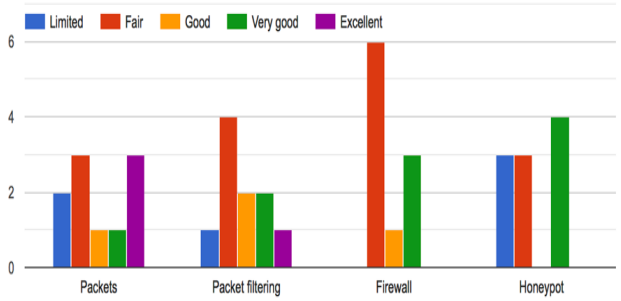

Fig. 4. Teachers' Perceived Levels of Knowledge (Post-Survey).

The same question was asked on both pre and post surveys and is listed at the top of the figure. In both figures, the y-axis shows the number of teachers and the color, knowledge level ranking. Ten teachers took part in our experiments.

We examined overall trends in the data, which showed 11 instances of growth of perceived knowledge and one instance

of a decline.[1] This indicates that after playing NetDefense, teachers felt that they were overall more knowledgeable about cybersecurity concepts. As we looked at the data in-depth, we also looked at specific changes in perceived knowledge to target which concepts NetDefense may be most and least helpful in aiding players' understanding of concepts. One participant changed their knowledge level on packets from "good" to "very good," and another changed their knowledge level from "very good" to "excellent." With packet filtering, two teachers changed their knowledge level from "limited" to "fair," one changed their level from "good" to "very good," and another changed their level from "very good" to "excellent." With "firewall," three teachers changed their knowledge response from "good" to "very good." With honeypots, one teacher changed their knowledge from "fair" to "limited" (the only regression of knowledge reported), one teacher changed from "fair" to "very good," and two students changed from "good" to "very good." This indicates that overall, the game seemed to assist the development of knowledge across concepts.

We also asked teachers specifically how they felt NetDefense contributed to their cybersecurity knowledge (see Figure 5). From the question in the figure, we find that in terms of NetDefense's contribution to teachers' cybersecurity knowledge, most teachers $(7/10)$ felt that playing the game had some significant contribution to their knowledge. Half of the teachers ranked NetDefense's contribution to their knowledge as $3/5$, demonstrating a moderate level of contribution to their knowledge

Fig. 5. Perceptions of NetDefense's contribution to building cybersecurity knowledge.

B. Teachers perception of NetDefense Utility

Prior to playing NetDefense, Figure 6 shows that 9 participants believed students could learn cyber security concepts from a game and one participant was unsure.

After playing NetDefense, participants were asked if students could learn cyber-security concepts from NetDefense. Figure 7 shows that nine teachers reported some version of

[1]Note that a teacher may report knowledge growth in more than one area of knowledge.

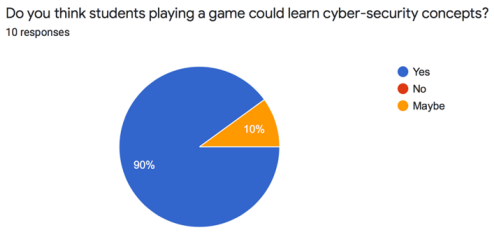

Fig. 6. Pre-survey on whether games (in general) could help students learn cybersecurity concepts.

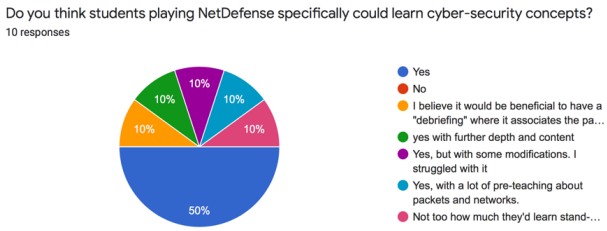

Fig. 7. Post-survey on whether NetDefense could help students learn cybersecurity concepts.

"yes." Five said yes without caveats, while four said yes with some changes. One suggested a debriefing, one suggested more depth, one suggested pre-teaching or activities, and one suggested general modifications. One participant said that they weren't sure how much students could learn from a game. This seems to indicate that playing the game solidified participants' earlier views that yes, students could learn cyber security concepts by playing NetDefense. We have already incorporated some of their suggestions and are in the process of incorporating others in order to improve the game and make it more suitable and effective for classroom inclusion. We find it encouraging that most teachers either said yes or were engaged enought to make suggestions for improvement.

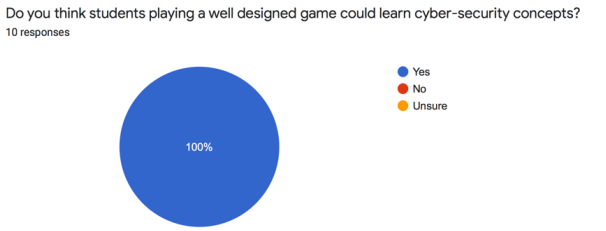

Fig. 8. Post-survey on whether a game could help students learn cybersecurity concepts.

Figure 8 does indicate that all teachers now believe that a well designed game could teach cybersecurity concepts. Since good game design depends heavily on user feedback, we expect NetDefense will benefit from such feedback and gain more usage and utility in classrooms and labs. This indicates

that to us, with time and feedback, NetDefense could be an appropriate tool for this type of learning.

C. Student Motivation and Learning

Prior to playing NetDefense, teachers ranked their perceptions of students' levels of motivation in learning about or using cyber security concepts on a scale from 1-5. Figure 9 shows that three teachers said $2/5$, four said $3/5$, two said $4/5$, and one said $5/5$. The average was .62 or approximately $3/5$.

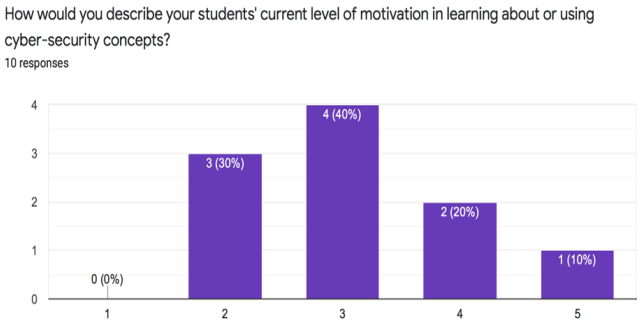

Fig. 9. Pre-survey on student motivation with respect to cybersecurity concepts

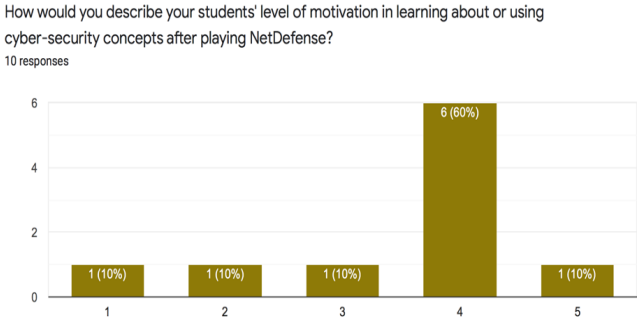

Fig. 10. Post-survey on teacher perception of student motivation after playing NetDefense.

Figure 10 shows that after playing NetDefense, teachers' overall perceptions of student motivation increased. The average was $7/10$, or $3.5/5$. The increase in average perception of NetDefense's utility is also encouraging and indicates that teachers believe that playing the game may motivate This demonstrates that playing the game may increase students motivation to become more interested in these concepts.

D. Discussion

We believe these results show that a game like NetDefense has the potential to play a significant role in addressing cybersecurity skills needed to protect privacy, identity, and personal information online. Starting with simple knowledge of data packets, routers, filtering and firewalls enables players (students and teachers) to build up a strong foundation for more complex technical concepts. We are designing and planning to conduct experiments with students to study impact on learning and motivation. This new data will provide better, more robust, statistically more significant analysis of such NetDefense's potential impact and usefulness.

We also note that although a game like NetDefense does not address social engineering and non-technical aspects of cybersecurity, it does, for example, implicitly teach about the existence of sources (and destinations) for malicious data packets. This is proximal to learning about and addressing ethical and social cybersecurity issues concerned with malicious or gullible human sources and destinations. Extending the game and more experimentation and data gathering will be needed to examine and analyze such impact.

VI. Conclusions and Future Work

This paper introduced a novel tower defense genre based game, NetDefense, for helping motivate and teach networking cybersecurity concepts. The game based approach is useful not only to help teach cybersecurity principles to K-12 students but also serves as a basis for further research in game based learning. playable version of the game, the github respository of source code, and a link to a video playlist showing gameplay.

- Play the game at:

  https://www.cse.unr.edu/ sushil/NetDefense2/
- The Github repository for downloadable source code is at:

  https://github.com/sushillouis/NetDefense
- Video tutorials and gameplay are at the cybersecurity playlist on the Evolutionary Computing Systems Lab (ECSL) youtube site:

  https://www.youtube.com/user/ecsllab/playlists

Using our RET projects as a vehicle, we plan to ask teachers participating in our RET summer programs to disseminate and test the NetDefense game in their classrooms and provide feedback. Initial studies with RET teachers have led to several positive findings. Based on these findings, we believe that NetDefense increased teachers' own perceived knowledge of concepts, solidified their beliefs that game-based learning can aid students in learning key cybersecurity concepts, and increased teachers' perceptions of student motivation. Additionally, teachers' provided excellent data regarding what could be improved or tweaked to make NetDefense an even more effective tool in motivating students and helping them learn. We plan to improve the game using feedback from our participants, disseminate the open source, publicly available game to all interested educators for classroom and laboratory use, and gather more data from students and teachers on game effectiveness. This will enable us to begin addressing research questions

ACKNOWLEDGMENTS

This research is supported by the National Science Foundation (NSF) Award 1855159. This work is also supported in part by grant number N00014-22-1-2122 from the Office of Naval Research. The views, opinions, findings and conclusions reflected in this publication are solely those of the authors and do not represent the official policy or position of our sponsors.

REFERENCES

[1] P. W. J, *Media Literacy*. Paris, France: Sage Publications, 2018.

[2] J. E. Paulsen, M. B. Hazelett, and S. B. Schwartz, "Cied cybersecurity risks in an increasingly connected world," *Circulation*, vol. 138, no. 12, pp. 1181–1183, 2018.

[3] "Cyber crime costs projected to reach 2 trillion by 2019," https://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/#4460021d3a91, accessed: 2022-04-23.

[4] "Home depot admits 56 million payment cards at risk after cyber attack," http://www.huffingtonpost.com/2014/09/18/home-depot-hack_n_5845378.html, accessed: 2022-04-23.

[5] "Jpmorgan chase says hacking affected 76 million households," http://fortune.com/2014/10/02/jpmorgan-chase-disclosed-cyber-breach/, accessed: 2022-04-23.

[6] "Health data breaches sow confusion, frustration," http://usatoday.com/story/money/2015/04/14/hacking-health-data-privacy/25597337/, accessed: 2022-04-23.

[7] "Cyberattack on experian may affect millions of t-mobile customers," https://www.seattletimes.com/business/technology/cyberattack-on-experian-may-affect-millions-of-t-mobile-customers/, accessed: 2022-04-23.

[8] "The great bank robbery: the carbanak apt," https://securelist.com/the-great-bank-robbery-the-carbanak-apt/68732/, accessed: 2022-04-23.

[9] "'crash override': The malware that took down a power grid," https://www.wired.com/story/crash-override-malware/, accessed: 2022-04-23.

[10] R. Akiyoshi, D. Kotani, and Y. Okabe, "Detecting emerging large-scale vulnerability scanning activities by correlating low-interaction honeypots with darknet," in *2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC)*, 2018, pp. 658–663.

[11] R. Sabillon, V. Cavaller, J. Cano, and J. Serra-Ruiz, "Cybercriminals, cyberattacks and cybercrime," in *2016 IEEE International Conference on Cybercrime and Computer Forensic (ICCCF)*, 2016, pp. 1–9.

[12] Y. Liu, Y. Zhou, and S. Hu, "Combating coordinated pricing cyberattack and energy theft in smart home cyber-physical systems," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 37, no. 3, pp. 573–586, 2018.

[13] "Federal cybersecurity research and development strategic plan," https://www.nitrd.gov/cybersecurity/publications/2016_Federal_Cybersecurity_Research_and_Development_Strategic_Plan.pdf, accessed: 2019-02-14.

[14] Z. Zainuddin, S. K. W. Chu, M. Shujahat, and C. J. Perera, "The impact of gamification on learning and instruction: A systematic review of empirical evidence," *Educational Research Review*, vol. 30, p. 100326, 2020.

[15] S. B. Merriam, ". introduction to qualitative research," *Qualitative research in practice: Examples for discussion and analysis*, vol. 1, no. 1, pp. 1–17, 2002.

[16] B. J, *Mixing methods: Qualitative and quantitative research*. Routledge, 2017.