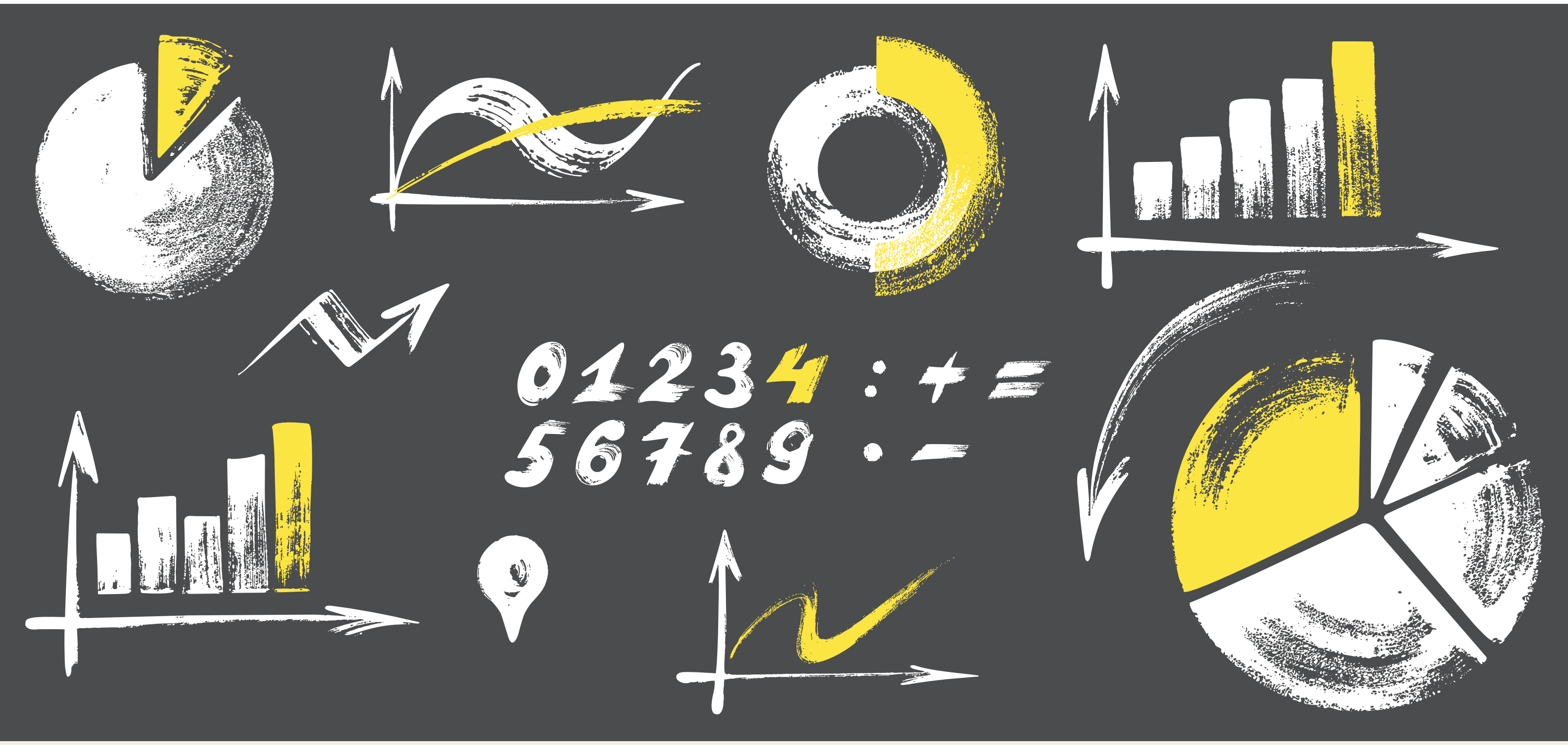
JOURNAL OF WOMEN AND MINORITIES IN TECHNOLOGY

ISSN: 2640-8015

Volume 1, Issue 3



As it did to other organizations and individuals, COVID-19 caused a disruption with our ability to publish this issue on time. However, we are grateful to the contributors who continued to work tirelessly on their submissions and our peer reviewers who continued to volunteer their time and expertise to make this issue possible. Our continued goal is to share timely information that is of interest to women and minorities interested in technical careers.

Founding Co-Editors: Jane LeClair, EdD and Tanis M. Stewart, PhD

Thomas Edison State University
School of Applied Science and Technology

Table of Contents

EDITORIAL BOARD

Founding Co-Editors

PEER REVIEWERS

The Women and Minorities in Technology Journal gratefully acknowledges the reviewers who have provided valuable service to the work development of the journal:

Peer Reviewers

Perpetuating Counternarratives to Societal Norms Through the Digital Sphere

Shantay Robinson

In *Habermas and The Public Sphere,* Nancy Fraser (1990) writes, "In stratified societies, subaltern counter publics have a dual character. On the one hand, they function as spaces of withdrawal and regroupment; on the other hand, they also function as bases and training grounds for agitational activities directed toward wider publics" (p.70). Black women as a subaltern group have successfully used the digital sphere to reclaim their power by creating virtual publics. By blogging, black women bloggers have created community for the purposes of empowering themselves and their followers. One such blog, which was established in 2006 is Afrobella. This blog has recently transformed from less of a singular blog presence to more of a multiple social media presence with each platform performing a different function. These days, the owner of the blog, Patrice Yursik has the most interaction with her following on social media platforms, particularly Instagram, Facebook, and Twitter with 215,000 friends on Facebook, 46,600 followers on Instagram with an average of hundreds of likes on Instagram for any post, and 92,500 followers on Twitter. Afrobella is an award-winning blog that Yursik states, "shines a loving light on natural hair and the wonderfully wide range of gorgeous skin tones and sizes women come in." Afrobella carves out space for a most marginalized group of women who do not represent the typical images of beauty promoted by mainstream media but a community who still wants to be recognized.

There have been attempts to counter the dominant culture's narratives of beauty by social media personalities, particularly by bloggers. But while some blogs are more successful than others in terms of empowering the audiences they serve, some who attempt to be progressive, only perpetuate the dominant narrative. According to Lynch (2011), author of "Blogging for Beauty? A Critical Analysis of Operation Beautiful," Operation Beautiful (OB), "was launched in 2009 with the mandate of improving women's and girls' self-esteem and body images" (Lynch, 2011, p. 583). Operation Beautiful's flaw was that it did not quite challenge the dominant narrative in being truly empowering. Elements of the blog that reinforce dominant narratives include the reference to toxic self-degradation as "fat-talk." While the participants of the blog use the term to admit to negative self-talk, the use of the word fat as a negative concept does little to change the dominant narrative. According to Harju and Huovinen (2017), Fatshion bloggers, on the other hand, have embraced the term fat and are using it as a form of resistance against societal norms. The use of the term "fatshion" has been helpful in gaining acceptance for diverse body sizes. These "fatshion" blogs are meant to empower marginalized groups while being subversive in the way they use hegemonic discursive practices to resist against dominant exclusionary practices.

Patrice Yursik, owner of Afrobella, is a full-sized woman with kinky hair who epitomizes some of the characteristic of her followers. She uses her presence to combat traditional perceptions of black women, as she suggests an alternative to those perceptions. Afrobella, is an empowerment blog by my estimates, in that it empowers black women with information they need to live their best lives and look their most beautiful while doing it. The brand's mission, to shine a loving light on many of the characteristics inherent to black women, performs the empowerment role in direct opposition to the dominant culture's definitions of those characteristics deemed attractive: long-blonde hair, fair skin, and slender figures. Afrobella promotes kinky natural hair, a range of skin tones and sizes. In a sense, she's renegotiating cultural norms by promoting body acceptance, economic and cultural empowerment, and combatting societal norms. Yursik's is an intersectional approach, as she is black, a woman, and plus-sized. She challenges the femininity and beauty ideals with her personhood. Through her blog, she promotes her whole self by often speaking of personal issues while at the same time promoting brands who are investing monetarily in black women. Afrobella has partnered with mainstream companies like MAC Cosmetics, Vogue, Essence, Ebony, and Newsweek. She was named one of Women's Wear Daily's 50 Most Influential People in the Multicultural Beauty Market in 2015. She is regularly sponsored by popular brands like Target and Eloqui. Harju and Huovinen (2017) note that "in order to gain acceptance, marginalized groups still need to show affiliation with privileged groups" (p. 1606). By Yursik's work of promoting the products of major corporations, she's earned an identity for herself and her followers.

Harju and Huovienen's (2017) study about fatshion blogs deemed that while they seem to attempt to be normative and conformists, they are actually resisting cultural norms by enabling marginalized people entrée into the mainstream. They make the claim that resistance and conformity are intertwined. These alternative sites mimic the dominant tropes of fashion blogs and at the same time negotiate consumerism. The dominant fashion world is only now starting to openly cater to people of various sizes. Blogs like Afrobella have identified and filled a gap by appealing to an audience who have not traditionally been represented. The popularity of these blogs could likely be the reason for the slight turn in corporate attention being paid to people of various sizes. Bloggers like Yursik have substantial followings indicating there is a need for this attention to consumers of diverse identities.

Black women as a group of consumers are marginalized and typically not seen as having substantial buying power. Harju and Huoivenen (2017) note that marginalized groups "are positioned as disadvantaged not only relative to available material resources due to limited market offering, but also regarding cultural and social resources" (p. 1606). Through blogging, Yursik is achieving social capital, cultural capital, and symbolic capital not only for herself but for the women she represents. The partnerships Yursik has with major brands implies that these brands are interested in black women as customers. The knowledge that her followers get from her blog on how to look and feel their best selves translates into opportunities for them in their real lives. And their reputations as women of class and distinction from the way they look and feel can change dominant perceptions of black women overall. Yursik places herself among her followers as an arbiter of good taste, and as superficial as that may seem, Harju and Huovienen (2015) state, "displays of good taste and cultural knowledge of fashion are vital in the identity construction of a group usually marginalized in the realm of fashion" (p. 1607). The knowledge of fashion and its norms is vital for the community Yursik serves if they want to be considered a more substantial part of society. When they look the part, they have better odds at performing a role.

While many of Afrobella's posts are about beauty products, fashion for plus-sized women, and general lifestyle topics, it exists in a realm of blogs targeting black women that empowers them with information they can use to live their best lives. Other bloggers that might exist in the empowerment blog realm are fitness blogger, Erika Nicole Kendall, beauty blogger Brittany Minor, and fashion blogger Gabbi Gregg. While these bloggers primarily use the blog as a medium, the genre they work in might be hybrid in that they exist as beauty, fashion, and fitness blog, but at the same time they are empowering black women who are typically ignored by mainstream media. Although these bloggers might not outwardly be actively denouncing dominant cultural norms, their attention to black women and the issues they face allow them to empower black women with knowledge on how to live transformative lives. In her essay "'Telling Our Own Stories': African Women Blogging for Social Change" on the motivations African women bloggers, Oreoluwa Somolu analyzes 92 blogs in African countries. She writes, "Many women capitalize on the ability of blogs to be 'a powerful conversational tool with the potential to reach a wide audience' and to 'empower by giving a voice to the unheard'" (2017, p. 483). Some of the women bloggers she studied were feminists who were actively using their blogs to speak to women in meaningful ways. Blogs thrive on the interaction between blogger and audience.

While there has been some conflict on whether blogs are a medium or genre, the consensus states that blogs are a medium, but that there are several genres of blogs (Primo et al., 2013, p. 344; Lomborg, 2011, p. 59). "If personal blogs were the only type of content available in the blogosphere, then blogs might be considered a genre in itself" (Primo et al., 2013, p. 44). Lomborg (2011) mentions "genre classifications are based on social conventions – genres are socially constructed and negotiated" (p. 57) and Primo et al. (2013) state "genre and medium, thus, should neither be confused not taken as synonymous" (p. 344). Lomborg (2011) states, "A genre comprises a class of communicative events, the members of which share some set of communicative purposes" (p. 62). A typical convention of blogs Schmidt (2007) identifies is, "…speaking in one's own personal voice and being open for dialogue rather than engaging in one-way communication…be it private online journals, corporate blogs, or political blogs" (p. 1413). As a medium, blogs are different from most television and some radio shows in that it encourages participation on the part of the audience. According to Fieseler and Fleck (2013), social media "…are believed to reduce transaction and coordination costs, making it easier for like-minded citizens to come together around foci of interest" (p. 761). This idea that citizens come together around a similar interest is what activates a genre. Black women congregate around alternative media like blogs because mainstream media tend not to cater to them (Fiesler and Fleck, 2013, p. 761). While there are mainstream media outlets like Essence Magazine, BET, and TV One, they tend to perpetuate dominant cultural ideals in ways that are ostracizing to black women. Afrobella creates posts that typically speak to issues like fashion and beauty that help black women learn about the best brands and products for them, but she also inserts her personal voice and shares aspects of her life. Carolyn Miller (2004), on her discussion about blogging as social action, writes, “Is what is truly novel in the blog the ability to address simultaneously these dual yet mutually reinforcing purposes, to engage in self-expression *in order* to build community and to build community *in order* to cultivate the self?” (p. 10-11). Yursik does a good job of responding to her audience on the blog and other social media sites. On the surface the roles of these bloggers might seem superficial as they seem to navel gaze, but their stories are actually touching other people’s lives. When Yursik was away from the blog for some time between November 2018 and January 2019, her community was comforting and respectful in her time of need.

Lomborg (2011) notes, “social media are distinctly social because they are based on interpersonal communication and interactive content creation, typically with a personal purpose” (p. 56-57). To have the interactivity necessary for the purposes of the blog, the owner of the blog needs to cater to their audience. Afrobella’s purpose is to carve out a space for black women to receive the care they need to live fruitful lives. Afrobella explores women’s lives by encouraging them to join the blogosphere and promote empowerment through the promotion of products many of which are created by black women. Somolu (2017) also writes, “empowerment implies enabling people towards self-determination and for women, this emphasizes the importance of increasing their power and taking control over decisions and issues that shape their lives” (p. 483). While it might be Yursik’s goal to “shine a loving light on natural hair and the wonderfully wide range of gorgeous skin tones and sizes women come in” (Afrobella), she is not explicitly writing about varied skin tones and the range of sizes women come in. Although her blog has become very commercial in that her posts typically mention a sponsor in some way, she is offering her followers tools with which to change the negative perception of black women.

Afrobella’s most interactive blogs are a list of 101 black-owned businesses, new hair products, and a natural hair shopping guide. So, typically Afrobella is best used as a resource guide for helping its following determine where to shop and what to buy. If the most commented blog posts are those of product giveaways and product recommendations, then she in a way is empowering her audience with goods and services they want. The most commented on posts, other than product giveaways, is on things black women can buy. It seems as though Yursik understands the wants of her audience, as she regularly posts articles about hair and beauty products since that is what her audience most interacts with in an effort to build community. While she may not be empowering them with writing about black hair, various skin tones, and diverse body sizes, Yursik is not only empowering herself and her followers, but also the brands she promotes; many of those are black owned businesses that cater to black women.

References

Fieseler, C & Fleck, M. (2013). The pursuit of empowerment through social media: Structural social capital dynamics in CSR-Blogging." *Journal of Business Ethics*, *118* (4), 759-775.

Fraser, N. (1990). Rethinking the public sphere: A contribution to the critique of actually existing democracy." *Social Text*, *25/26*, 56-80.

Harju, A. & Huovienen, A. (2015). Fashionably voluptuous: Normative femininity and resistant performative tactics in Fatshion Blogs. *Journal of Marketing Management*, *31*, (15-16), 1602-1625.

Lomborg, S. (2011). Social media as communicative genres. *Journal of Media and Communication Research*, *51*, 55-71.

Lynch, M. (2011). Blogging for beauty? A critical analysis of Operation Beautiful. *Women's Studies International Forum*, *34*, 582-592.

Miller, C. (2015). Genre as social action (1984), Revisited 30 years later (2014). *Letras & Letras*, *31*(3), 56-72.

Miller, C. (2004). Blogging as social action: A genre analysis of the weblog. *Into the Blogosphere*, *18*(1), 1-24.

Nardi, B., A., Schiano D., & Gumbrecht, M. (2004). Blogging as social activity, or, would you let 900 million people read your diary? CSCW '04 Proceedings of the 2004 ACM Conference on Computer Supported Cooperative Work. *Letters Chi*, *6*(3), 222-231.

Primo, A., Zago, G. Oikawa, E. & Consoni, G. (2013). The Post as an utterance: Analysis of themes, compositional forms and styles in blog genre studies. *Discourse & Communication*, *7*(3), 341-358.

Schmidt, J. (2007). Blogging practices: An analytical framework. *Journal of Computer-Mediated Communication*, *12*, 1409-1427.

Somolu, O. (2007) 'Telling our own stories': African women blogging for social change." *Gender and Development*, *15*(3), 477-489.

About the Author

Shantay Robinson

Shantay Robinson is a doctoral student in the Writing and Rhetoric program at George Mason University where she has taught Composition, Writing for Artists, and Professional and Technical Writing. Her interests include multimodal composition, visual rhetoric, and black feminist theory.

Maritime Autonomous Vessel Cybersecurity: Not the Time to Rush Implemental

Charles Parker, III, Ph.D

Cybersecurity Application

Earlier this year, Europe was preparing for autonomous shipping and ports to accept these ships and cargo, which was based on the Project AUTOSHIP (Autonomous Shipping Initiative for European Waters) report (Felski, & Zwolak, 2020; Bolbot, Theotokatos, Boulougouris, & Vassalos, 2019; Bolbot, Theotokatos, Boulougouris, & Vassalos, 2020; Gu, Goez, Guajardo, & Wallace, 2020). The report's focus was to increase the pace for transitioning from the present protocols to the autonomous form factor. This is a relatively new topic of research and application as autonomous maritime applications have only been within the last five to ten years a potential application. Prior to this, the technology simply was not to a point of maturity to a real-time application in a vessel, versus in comparison to a proof-of-concept (PoC) project. In 2010, certain modules were in use, however, not an autonomous system in an entirety. An example of this the use of autonomous GPS (Hassani, Crasta, & Pascoal, 2017). While the importance of GPS was noted, the cybersecurity was likewise researched as a critical failure point. For the autonomous vessel to be successful, it has to be fully secured with tested and approved cybersecurity in place. If the vessel were to receive false GPS data, as in the case of spoofing, the result could be a disaster. This was likewise researched by Elkins, Sellers, and Monarch (2010), however they also looked at the effect of not only the GPS, however, other sensor's data being fused together. The COLREGs-compliant algorithms for autonomous vessel navigation has been researched as alternatives (Naeem, Henrique, & Hu, 2016; Kuwata, Wolf, Zarzhitsky, & Huntsberger, 2014). The attacks may lead to ransomware for the ship's OT and the ship itself. As this relates to the cargo, this type of theft has been an international issue (Yang, Ballot, & Cedillo-Campos, 2018; Ship Technology, 2017).

The maritime industry has addressed the issue since at least 2002 with the Maritime Transportation Security Act (Shah, 2004). The regulation was created from the need to identify the potential vulnerabilities of the vessels and ports and addressed, among other topics, applying cybersecurity to vessels and their operations. While significant attention was placed on the topic with the last 20 years, the Maritime industry is still vulnerable to cyberattacks (Caponi, & Belmont, 2015). Depending on the types of attacks, the attacker may follow various levels of cybersecurity compromise from a module or individual system enabling them to commandeer a vessel. The attack would affect the vessel, cargo, and its data.

There have been several successful proof-of-concept (PoC) attacks targeting maritime cybersecurity. One of these occurred in 2013, when the cybersecurity team from the University of Texas-Austin secured the vessels navigation via spoofing the global positioning system (GPS) (DiRenzo, Goward, & Roberts, 2016). The focus on maritime cybersecurity is very appropriate, given the risks involved such as if a cargo ship or other vessel is successfully attacked by cyber means. The issue has been and continues to lag behind the level of application which should be applied for cyber protection of autonomous shipping to be implemented. Maritime pirates have also explored ships and vessels that are lacking cybersecurity implementation in the maritime sector (Frodl, 2012).

Prior Research

Securing Shipping Containers

Vannieuwenborg, Lannoo, Verbrugge, and Colle (2016) researched the use of smart containers in the effectiveness of goods and processes dependent on this shipping mode. The monitoring provided the platform for observing additional work with the product and container. Their research indicated when a container arrived in port, and how there is a significant amount of time prior to the container continuing to move through the processing. The research indicated that using these smart containers would decrease the processing time, which would increase the impact and the number of containers that are able to be shipped and processed.

Cargo Theft

Cargo theft is a significant issue across the globe. This is prevalent to the point Lorenc and Juznar (2018) researched methods to predict the estimated risk and cost of these thefts, however they were measured based upon roadway incidents. The research was further based on simulating the different forms of cargo, costs, and stage of delivery. The analysis of the research was based on the researcher's algorithms that were applied to artificial neural networks (ANN) for analysis. The ANN's analysis provided for the predicted loss values based on the type of the cargo stolen. The research was based on these algorithms in a simulation; however, the research did not provide a base of work to continue. The pirates have also been using internet technology to search for any information on the ships including the cargo that was being shipped, ship locations, and other data points (Frodl, 2012). These data points were part of OSINT (open source intelligence), could be used to track and possibly later commandeer the ships and ask for ransom for the cargo, ship, or crew if present.

Automated Identification System (AIS)

AIS is used for vehicle identification and provides for an extended attack surface (Balduzzi, Pasta, & Wilhoit, 2014). The researchers analyzed the potential vulnerabilities and found several threats. These included ship spoofing, AtoN spoofing, collision spoofing, AIS-SART spoofing, weather forecasting, AIS hijacking, availability disruption threats, and other issues with the software, hardware, and radio frequencies. These are valid threats and vulnerabilities to conduct attacks on this mandatory and valuable system.

Autonomous Maritime Navigation Systems

Navigation systems working as engineered are clear requirement to automate processes, as much as possible, this aspect of the OT (operating technology) continues to be designed with the intent of being part of the autonomous vessel. The autonomous marine navigation (AMN) systems were researched by Hassani, Crasta, and Pascoal (2017) as integral to the OT system along with the cybersecurity shortfalls. In particular, the researchers analyzed the scenario such as if the attacker were to block the real GPS signal and replace it with false signals. In addition to the sensors and their respective data, other researchers have also researched the algorithms used with autonomous navigation systems. These algorithms were coded to comply with the

International Regulations for Preventing Collisions at Sea (COLlision REGulationS (COLREGs)) (Kuwata, Wolf, Zarzhitsky, & Huntsberger, 2014; Naeem, Henrique, & Hu, 2016).

Systemic Cybersecurity

The application of cybersecurity to the maritime systems was researched to gauge its level of maturity (Caponi & Belmont, 2015). As the maritime industry is one of the earliest transportation systems still in place and viable, it is coupled with the responsibility and risk of vast amounts in volume and value which is transported by these vessels every single day. The data to be also protected within each vessel should be a natural application for cybersecurity capabilities. Reports have noted the Maritime industry is however just as susceptible to cybersecurity risks as others. Other researchers have also noted maritime cybersecurity has not been researched to its appropriate extent (DiRenzo, Goward, & Roberts, 2015). The lack of research in this area of maritime cybersecurity is alarming, as successful attacks have immediate, far reaching and more costly effects.

This is not a new application for cybersecurity. In 2004, this was examined by Shah (2004). At that junction, the researcher reviewed the state of maritime cybersecurity regulations and its statutes. The Maritime Transportation Security Act (MTSA), was signed into actionable law on November 25, 2002, and it addressed the issue to a very limited extent. The act included requiring U.S. ports to have in place a thorough security plan, the requirements to improve the identification and screening of seaport personnel, to increase and better the maritime domain awareness, and to improve the level for international port security.

Autonomous Shipping

Autonomous shipping will be a reality. However, the timing will be an issue. In the case of autonomous shipping being implemented too quickly, without the requisite cybersecurity vetting, testing, and governance, the potential of the vessels hardware and/or operations to be successfully attacked will be very significant. The vessel would act as the target to be compromised and provide the venue for attacker's to use and perfect their attack methodologies on any new platform. The risks associated with the overly ambitious autonomous vessels by far outweigh the potential benefits.

The conservative approach will provide the balance for cybersecurity to be implemented throughout the system, in comparison to being applied too late in the project to be effective. Waiting until the risks substantially have been mitigated is the wiser route to take. In the case where the vessels have the autonomous shipping implemented without having fully applied cybersecurity, the attack surface will be rather substantial. In this scenario, modules were used for the attack of the systems such as communications, and inter-system communications, at a minimum. Once the attacks are launched and are successful the attacker could have control over the entire ship's systems and are able to manipulate the systems as they desire.

Analogy by Proxy

In order for others to learn from others missteps and oversights, experience should provide a reduction in the learning curve. There are other industries which have previously and are currently working through the autonomous aspect and applying cybersecurity to ensure the mitigation of potential attacks. While these industries and systems are precisely the same, the learning experiences provide the opportunity not to repeat the same missteps of the industries using the autonomous features such as the predominant and most likely automobile manufacturing industry.

Connected and Autonomous Vehicles (CAVs)

The automobile manufacturing industry is working diligently to implement the autonomous drive vehicle to be driven throughout the globe. The vehicles in use presently are connected, which continues to grow in depth and in complexity. These vehicles provide many features for the consumer and commercial clients in which to use. While completely different modes of transportation, the maritime and vehicle industries are related in theory and in applications. Both the automobile and maritime vessels communicate from remote locations. However, vehicles presently communicate in limited applications and are more utilized. However, in the future there will be the vehicle-to-infrastructure (V2I) and dedicated short range communication (DSRC) systems for more advanced communication systems (3M, n.d.). Vessels likewise are required to communicate from their remote locations for updates and with their Automatic Identification System (AIS) (Balduzzi, Pasta, & Wilhoit, 2014). The interaction process communicates the GPS coordinates via radio transmissions. The vessels may be tracked via the internet (Marine Traffic, n.d.).

The maritime vessels also use multiple sensors to provide data to their respective operating systems. The collected data is fused together for analysis for logging, decision-making, and other functions. In a vehicle, the data may, dependent on the model and manufacturer, GPS, cameras, LiDAR, and RADAR. Vessels use primarily the same sensors (Elkins, Sellers, & Monach, 2010). In addition, the vessels use to vibration modules and sensors, among others.

The industries likewise require cybersecurity to be applied to their industry. Without this fully implemented, the issues would be immediate as the attackers would gain their unfettered access quickly and more effectively. As there are commonalities, the maritime industry has the option to learn from the challenges experienced by the automakers to gain knowledge of what to avoid. The vehicle attacks date back to at least 2002 with the VW and Audi attacks, and the infamous 2015 FCA Jeep hack (Tengler, 2020). These vulnerabilities are still present within the vehicle embedded systems. The published attacks and proof-of-concept (PoC) attacks provides direct evidence of the issues and the opportunity to learn from their oversights.

The automobile and maritime vessel industries are different, yet have many similarities with their embedded systems, which provides a platform for the maritime system to learn. The industries use the same types of sensors, communication outside of the vehicle/vessel, embedded systems, and commonly the same platforms for the modules to communicate with each other. The maritime industry should review the past cybersecurity performances in the vehicle industry for the application into their use cases. The successful attacks continue to haunt the industry as new issues arise from the newly developed hardware and software systems, and prior cybersecurity issues not previously resolved. The automobile systems are not ready for full autonomy yet. While the vehicle engineering has been making incredible strides, the automobile industry is not ready to be implemented a fully autonomous vehicle. The lacking cybersecurity applications and vulnerabilities that are currently present allow for a level of risk which is not acceptable. The automobile OEMs have been diligently applying their staff, engineering, and resources to solve this issue, which is still open and being worked on.

Discussion

The maritime industry has a multitude of targets and unfortunately the Maritime industry cannot hope that cyber attackers will not notice the wide target surface in which to protect. Security by obscurity rarely works. The stakes that are involved with maritime cybersecurity is very high and therefore, better cybersecurity protection should be a requirement to be fully and appropriately implemented.

The maritime industry must look to the automotive industry to understand the far-reaching effects from the lack of appropriate planning and implementation with cybersecurity, or the organizations will repeat these oversights. The issue with applying cybersecurity within automobile systems is very significant. Granted, maritime cybersecurity applications are more unique than the automobile industry. However, there are distinct commonalities as stated before with communication, embedded systems, and other system applications. While the autonomous vessel would not have a crew to be concerned for, the cargo, ship, and data still remain as targets. Therefore, a properly executed cyber attack could be orchestrated to commandeer the ship, remove the beaconing systems, and have the ship sail in a different direction and to a different location.

The cybersecurity has much further reaching implications not only for cybersecurity, however, for the maritime industry as a whole. If autonomous shipping is implemented too quickly with the focus of being the first to market, without the proper level and planning involved, the direct and significant economic impact will be felt immediately if the vessels are successfully attacked by cyber means. In the case of large cargo vessels, the cost of this would be massive. There is also the potential for successful cyber attackers to ransom the ship back to the owners for an appropriate price.

After the cybersecurity has been implemented for maritime applications, it will be difficult to know if the industry applied to proper risk mitigation to the scenario. If the maritime industry, however, does not apply the proper level of cybersecurity to its current vessels, the lack of application will be quite apparent.

References

3M. (n.d.). What is vehicle-to-infrastructure (V2I) communication and why do we need it? Retrieved from https://www.3m.com/3M/en_US/road-safety-us/resources/road-transportation-safety-center-blog/full-story/~/what-is-vehicle-to-infrastructure-v2i-communication-and-why-do-we-need-it/?storyid=021748d7-f48c-4cd8-8948-b7707f231795#:~:text=Vehicle%2Dto%2DInfrastructure%20(V2I)%20communication%20is%20the%20wireless,between%20vehicles%20and%20road%20infrastructure.

Balduzzi, M., Pasta, A., & Wilhoit, K. (2014). A security evaluation of AIS automated identification system. *ACSAC '14: Proceedings of the 20th Annual Computer Security Applications Conference*; December 2014.

Bolbot, V., Theotokatos, G., Boulougouris, E., & Vassalos, D. (2019). Safety related cyber-attacks identification and assessment for autonomous inland ships. *International Seminar on Safety and Security of Autonomous Vessels (ISSAV)*, 2019-09-17.

Bolbot, V., Theotokatos, G., Boulougouris, E., & Vassalos, D. (2020). A novel cyber-risk assessment method for ship systems. *Safety Science, 131*, doi:https://doi.org/10.1016/j.ssci.2020.104908. Retrieved from https://www.sciencedirect.com/science/article/pii/S0925753520303052

Caponi, S.L., & Belmont, K.B. (2015). Maritime cybersecurity: A growing threat goes unanswered. *Intellectual Property & Technology Law Journal, 27*(1), 16-18.

DiRenzo, J., Goward, D.A., & Roberts, F.S. (2015). The little-known challenge of maritime cyber security. *2015 6th International Conference on Information, Intelligence, Systems and Applications (IISA)*, 6-8 July, 2015. Doi:10.1109/IISA.2015.7388071

Elkins, L., Sellers, D., & Monach, W.R. (2010). The autonomous maritime navigation (AMN) project: Field tests, autonomous and cooperative behaviors, data fusion, sensors, and vehicles. *Journal of Field Robotics, 27*(6), 790-818. doi:https://doi.org/10.1002/rob.20367. Retrieved from https://onlinelibrary.wiley.com/doi/epdf/10.1002/rob.20367

Felski, A., & Zwolak, K. (2020). The ocean-going autonomous ship-Challenges and threats. *Journal of Marine Science and Engineering, 8*(1), 41. doi:10.3390/jmse8010041. Retrieved from https://www.mdpi.com/2077-1312/8/1/41/htm

Frodl, M.G. (2012). Pirates exploiting cybersecurity weaknesses in maritime industry. *National Defense; Arlington, 96*(702).

Gu, Y., Goez, J.C., Guajardo, M., & Wallace, S.W. (2020). Autonomous vessels: State of the art and potential opportunities in logistics. *International Transactions in Operational Research, 2020*, 1-34. doi:https://doi.org/10.1111/itor.12785

Hassani, Crasta, & Pascoal, A.M. (2017). Cyber security issues in navigation systems of marine vessels from a control perspective. *International Conference on Offshore Mechanics and Arctic Engineering, 2017*. doi:10.1115/OMAE2017-61771

Kuwata, Y., Wolf, M.T., Zarzhitsky, D., & Huntsberger, T.L. (2014). Safe maritime autonomous navigation with COLREGS, using velocity obstacles. *IEEE Journal of Oceanic Engineering, 39*(1), 110-119. doi:10.1109/JOE.2013.2254214. Retrieved from https://ieeexplore.ieee.org/abstract/document/6519944?casa_token=bo3oXr8FSgUAAAAA:qQxGuShmxk6nhJFKfTS4jb9Ao2GgqFac9g1eRaRCSv_nGkXG5eRdQr_U5Tax8ZUuyUQL3E93eQE

Lorenc, A., & Kuznar, M. (2018). An intelligent system to predict risk and costs of cargo thefts in road transport. *International Journal of Engineering and Technology Innovation, 8*(4), 284-293.

Marine Traffic. (n.d.). Live map. Retrieved from https://www.marinetraffic.com/en/ais/home/centerx:-85.6/centery:43.2/zoom:8

Naeem, W., Henrique, S.C., & Hu, L. (2016). A reactive COLREGs-compliant navigation strategy for autonomous maritime navigation. *IFAC-PapersOnLine, 49*(23), 207-213. doi:10.1016/i.facol.2016.10.344

Shah, S.K. (2004). The evolving landscape of maritime cybersecurity. *Review of Business; New York; 25*(3), 30.

Tengler, S. (2020, June 30). Top 25 auto cybersecurity hacks: Too many glass houses to be throwing stones. Retrieved from https://www.forbes.com/sites/stevetengler/2020/06/30/top-25-auto-cybersecurity-hacks-too-many-glass-houses-to-be-throwing-stones/#a78758e7f65d

Vannieuwenborg, F., Lannoo, B., Verbrugge, S., & Colle, D. (2016). Smart containers: Quantifying the potential impact. In *ITS Biennial (International Telecommunications Society) World Conference*, pp. 1-20.

About the Author

Charles Parker II, PhD

Charles Parker has over a decade of experience in the InfoSec industry beginning in the banking industry and continuing through the medical and vehicle industries. He focused on improving InfoSe environment through presenting on various subjects, writing extensively on cybersecurity Application and breaches and consulting. His current research projects are focused on vehicle, maritime, and satellite attacks, along with AI and quantum computing. Charles currently works at Stephenson Technology Corporation as a Senior Information Systems Security Engineer.

Mediating Effect of Attitude on Relevant Local Content and Gender Digital Inclusion in Uganda

Michael Koyola
Bonface Abima
Geoffrey Mayoka Kituyl
Robert Kyeyune
Bernard Engotoit

Abstract

Purpose: Developing countries are increasingly recognizing the potential of digital technologies in empowering women and helping them overcome some of the inequalities and barriers to opportunity that they face through enabling them to have access to information, opening new opportunities for income generation, facilitating their financial independence, engagement with community and political decision-making. However, this potential has not been fully realized in Uganda since women do not have the same opportunities to access and use digital technologies, and benefit from them, as men. Women in Uganda are not fully included in the information society and this is reflected by few females owning mobile phones, using computers and using the internet. Therefore, this study sought to examine the mediating role of attitude on the relationship between relevant local content and gender digital inclusion among women in Uganda.

Methodology: Quantitative research methods were used to collect, analyze and present the data. Survey questionnaires were used to collect data from a sample of 384 women across Uganda. Data were analyzed using frequencies, percentages, Baron and Kenny procedure for testing mediation, MedGraph and Sobel values.

Findings: Using MedGraph and Sobel values test, the findings reveal that attitude mediates the relationship between relevant local content and gender digital inclusion in Uganda.

Practical implication: The study therefore recommends that digital content should be created and localized to needs of women and in a language that they understand in order to improve their attitude towards adoption and use of digital technologies.

Originality/Value: The study provides evidence of the existence of an eminent problem of gender digital inclusion in Uganda with only 5.4% of the Ugandan women reported to have used a computer (Desktop, laptop or tablet) in 2018 and only 9.5% of the women having had access to and had used the internet in 2018. Limited studies have been conducted in Uganda to examine the issue of digital gender divide which is worrying and exacerbating existing socioeconomic gaps between men and women in the country.

Keywords: Relevant Local Content, Attitude, digital technologies, gender digital inclusion

Introduction

Digital technologies (DTs) are offering unprecedented new opportunities to meet vital development goals in domains such as education, financial inclusion, entrepreneurship, civic participation and a lifeline for critical health services and information than before across the globe. With specific focus to the female gender, the use of digital technologies has the potential, to empower women and help overcome some of the inequalities and barriers to opportunity that they face (International Center for Research on Women [ICRW], 2012). Souter and Anri (2018) argue that these digital technologies can; (a) aid women to access services and information formerly inaccessible to them; (b) open for them new income generating opportunities; (c) support them to attain financial independence; (d) foster them into personal development and (e) enable them to engage in socio-political decision-making in their different communities. Such opportunities can indeed positively impact individual women and the communities that they live which can subsequently contribute to the general development in the country.

Despite the above benefits that come with digital transformation, the use of digital technologies has not benefited all of human race. Studies by (Organization for Economic, Co-operation and Development [OECD], 2018; Information Telecommunication Union [ITU], 2016; Zhao, 2013) indicate that there is a significant gender gap in adoption and usage of digital technologies with the female gender having less access, use and ownership of these technologies as compared to the men. Global statistics indicate that 12% of the women are less likely to use the internet, with the situation on getting worse in low- and middle-income countries where 26% of the women are less likely to use mobile internet than men and 10% less likely than men to own a mobile phone (ITU, 2017). The worst cases are noticeably in Least Developed Countries (LDCs), where 33% of the women are less likely to use the internet.

Drawing specific attention to Uganda, this situation (Digital gender gap) is not any different, with reports indicating that few females own mobile phones, use computers and use the internet. For example, a National IT survey conducted by NITA-U in 2018 indicates that only 5.4% of the Ugandan women had used a computer (Desktop, laptop or tablet) in 2018. The survey further reports that in regard to internet access and usage, only 9.5% of the women had accessed and used the internet in 2018. This state of digital gender divide is worrying and exacerbating existing socioeconomic gaps between men and women in the country. This therefore means that Uganda will not be able to attain the United Nations Sustainable Development Goal 5b of using digital technologies to promote women empowerment and providing equal access to appropriate new technologies by 2030. This scenario implies that many women and girls in Uganda will continue to lack access to life-enhancing information, hence hindering the objective of reducing poverty and attaining inclusive economic growth. This study therefore seeks to examine the mediating role of attitude on the relationship between relevant local content and Gender digital inclusion in Uganda through the following hypothesis;

H1: Attitude positively mediates the relationship between relevant local content and gender digital inclusion in Uganda.

Conceptual framework

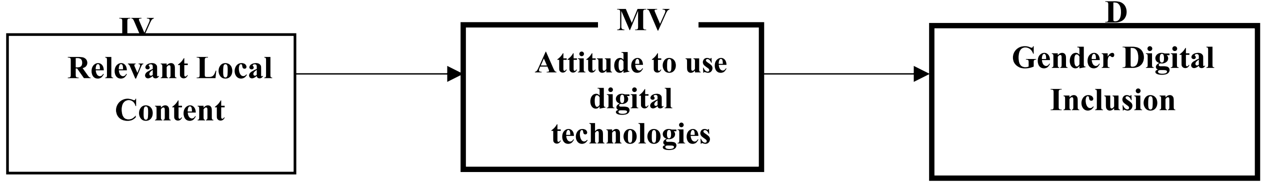


Figure 1. Conceptual framework. Adopted from Davis, Bagozzi & Warshaw (1989), Davaki, (2018), ITU, (2017), Davaki, (2018)

In this conceptual framework, Relevant Local Content is an Independent variable (IV), Attitude is a Mediating variable (MV) whereas Gender digital inclusion is the dependent variable (DV). Attitude is hypothesized to have a positive mediating effect on the relationship between relevant local content and gender digital inclusion in Uganda.

Literature

Theoretical grounding

This study bases on the modified Technology Acceptance Model by Davis, Bagozzi & Warshaw (1989) to ground Attitude as a mediating variable. In this modified model, Attitude alongside other variables like perceived ease of use, perceived usefulness and external factors are confirmed to influence behavioral intention to use and the actual usage of the system. Davis, Bagozzi & Warshaw (1989) therefore argue that there exists a strong positive relationship between attitude towards use and adoption of a new technology. On the other hand, Relevant Local Content and Gender Digital Inclusion are extracted from other extant literature reviewed (Davaki, 2018; ITU, 2017; Davaki, 2018).

Relevant Local Content, Attitude of women towards use of digital technologies and Gender digital inclusion

According to Ajzen and Fishbein (2005), attitude is an important concept that is often used to understand and predict people's reaction to an object (such as ICT) or change and how behavior can be influenced. Therefore, Velnampy (2008) define attitudes as feelings and beliefs that largely determine how people will perceive their environment, commit themselves to intended actions, and ultimately behave. Such feeling and beliefs influence how individuals relate to all objects and situations to which it is related. Borrowing from the definition above, with specific interest to digital technology, attitudes towards using digital technologies can be defined as an "individual's feeling beliefs about using digital technologies.

As far as adoption and usage of digital technologies is concerned, studies have shown that more women than men have been affected by attitudinal factors (Varank, 2007; Colley & Comber, 2003). The researchers argue that women have a negative attitude towards ICT and therefore tend to like and use computer less (Colley and Comber, 2003), feel less comfortable with computers

(Cooper and Weaver 2003) and are less likely to enjoy and feel less involved with computers than men do (Mucherah, 2003). Women actually perceive that their abilities are significantly lower than men's (Cooper, 2006; Correa, 2010; Hargittai & Shafer, 2006), which eventually may affect their motivation towards using digital technologies. Such negative attitudes discourage women from being included in the digital world thus widening the gender digital gap. Cunningham (2007) argues that this can lead to many socio-economic consequences such as limited employment opportunities, limited participation in the information economy, limited participation in democratic society as well as limited participation in ICT oriented classroom/training activities.

It is noted that the biggest challenge for women participating in the digital sector is that digital content is often not tailored to women and thus leave out topics of interest to them. A report by ITU (2017) explains that a number of women who are not connected to the internet feel that they will gain little value from internet access or content, while others do not make more extensive use of the internet due to the lack of relevant content tailored to women.

Hence H1; *Attitude has a positive mediating effect on the relationship between relevant local content and gender digital inclusion in Uganda.*

Methodology

A cross-sectional field survey design involving data collection and analysis was used and thus a quantitative approach involving quantitative research techniques (self-administered questionnaires) were used during data collection. Prior to the survey, a pilot study was carried out, and questionnaires were tested for reliability and validity among a section of the intended respondents. The questions tested for validity where presented on a five-point likert scale of (1 = Not relevant, 2 = Somewhat relevant, 3 = Quite relevant, 4 = Relevant and 5 = Very relevant) and distributed to expert judges to test for validity of the questions asked on each variable and whether they investigate what they intent to measure. This is in line with Carcary (2008) who states that a research instrument used to collect data should be valid in terms of the content covering a representative sample of the behavior domain to be measured. Content validity index (CVI) was used to test for validity of the research instrument and results revealed a CVI of 0.71 which according to Polit et al. (2007) is acceptable. Reliability tests were carried out using Cronbach Alpha Coefficient to ensure validity of the questionnaire instrument. This is in line with (Saunders & Lewis, 2009) who states that a research instrument used to collect data should be able to yield similar results at all the time. The pilot study test results for reliability indicated that the questionnaire items analyzed using Cronbach's alpha coefficient were found to have a coefficient of 0.70 and above which is also acceptable in research Nunnaly (1978).

The study population included Women in Wakiso district (Central Uganda) and Mbale district (Eastern Uganda). The Uganda Bureau of Statistic [UBOS] (2017), citing from the National Population and Housing Census (2014) states that the population of women in Wakiso district was estimated at 1,054,919 while that of Mbale district was estimated at 255,194. This therefore makes the total population for this study to be at 1,310,113 for both Wakiso district and Mbale district. Wakiso district was chosen because has the highest population of women living in it thus making it even ease to access data. However, considering that Wakiso district is largely an urban setting, the researcher also felt it necessary to capture views of women from a rural setting. Therefore, to serve that purpose, Mbale district in Eastern Uganda was chosen. A total of 384 respondents out of a population of 1,310,113 respondents in Wakiso district and Mbale district were selected. The sample size of the respondents was selected based on Krejcie and Morgan, (1970) table of sample size selection. This is also supported by McCall (1994) who states that a researcher needs to get the appropriate sample size in terms of accuracy and cost and that for any population size that is one million (1,000,000) and above, the sample size is constant (384). A simple random sampling method was adopted in order to get representative views of the respondents in the two selected districts where the study will be conducted.

Primary data was directly collected from respondents through administering a structured questionnaire. These primary respondents included girls and women in different sectors of the economy such as educational institutions, business sector, informal sectors, and formal sectors among others, which are affected by the digital transformation. The researcher employed services of a research assistant who was closely monitor during data collection. Secondary sources will include published journals and other scholarly materials on each study variable. The primary data related to the study variables as captured through administering questionnaires. The questionnaire was composed of questions relating to use of Relevant Local Content, Attitude towards use of digital technologies and Gender Digital Inclusion among the women in Uganda. Secondary data was obtained through literature review of the previous research findings and existing literature on each study variable.

All variables including relevant local content, Attitude and the dependent variable Gender Digital Inclusion were measured on interval scales derived from previous studies as shown in Table 1 below. These measurements were anchored on interval scales of I to 5, with Strongly Agree on 1 and Strongly Disagree on 5.

Table 1. Measurement of variables

Variable	Measurement	Source of measurement
Relevant Local Content	• Usefulness of digital content • Language for creating content • Level of involvement	(Microsoft, UNESCO, United Nations Women & ITU 2014 and Patil, Dhere & Pawar, 2009)
Attitude	• Affective- feelings toward digital technologies • Individual Perceived Usefulness of digital technologies • Perceived Control (perceived comfort level or difficulty of using digital technologies)	The Computer Attitudes Scale (CAS) (Selwyn, 1997)
Gender Digital Inclusion	• Affordable access to digital technologies • Use of digital technologies	Davaki (2018).

During processing, analysis and presentation of data, the collected data was coded, edited for incompleteness and inconsistence to ensure correctness of the information given by the respondents. Data was tabulated and input in the Statistical Package for Social Science (SPSS). Descriptive statistics using frequencies and percentages were used to present the respondents background statistics. Baron and Kenny (1986) procedure for testing mediation was also used to determine the mediation effect of attitude in the relationship between Relevant Local Content and Gender Digital Inclusion of women in Uganda. Further, results from correlation and regression analysis were entered into the MedGraph by Jose (2013) in order to determine the direct, indirect and total effects as well as Sobel values.

Ethical considerations

Since the research involves human subjects, there is need to pay attention to ethics. Participants were asked to participate freely and they were assured of confidentiality and privacy of their information. Ethical aspects such as consent, confidentiality and voluntary participation were observed during the study.

Results

Sample characteristics

The sample characteristics of the respondents included age, marital status, level of education and occupation. Age was considered because according to literature, the younger generations are likely to use digital technologies. Marital status was considered because spouses sometimes influence the use of digital technologies, level of education was analyzed given that digital literacy is considered as one of the prerequisites for women to comfortably use digital technologies and finally occupation was analyzed to find out which category of women in terms of employment status are likely to use digital technologies. These were analyzed and presented in a table using frequencies and percentages as shown in table 2 below.

Table 2: sample characteristics

Age category	**Frequency**	**Percent**	**Cumulative Percent**
18-25 years	65	20.4	20.4
26-30 years	156	48.9	69.3
31-35 years	61	19.1	88.4
36-40 years	26	8.2	96.6
40 years and above	11	3.4	100.0
Total	319	100.0	
Marital status			
Married	153	48.0	48.0
Single	166	52.0	100.0
Total	319	100.0	
Level of education			
O-level	40	12.5	12.5
A-level	60	18.8	31.3
Certificate	54	16.9	48.3
Diploma	47	14.7	63.0
Degree	108	33.9	96.9
Masters	8	2.5	99.4
Ph.D.	2	.6	100.0
Total	319	100.0	
Occupation			
Student	20	6.3	6.3
Self-employed	89	27.9	34.2
Unemployed	71	22.3	56.4
Employed in the private sector	70	21.9	78.4
Employed in the government sector	69	21.6	100.0
Total	319	100.0	

Testing for mediation

Baron and Kenny (1986) procedure for testing mediation was used to determine the mediation effect of Attitude on the relationship between Relevant Local Content and Digital Gender Inclusion of women in Uganda. Further, results from correlation and regression analysis were entered into the MedGraph by Jose (2013) in order to determine the direct, indirect and total effects as well as Sobel values. The results are presented as follows: -

Correlations and regressions of relevant local content, attitude and gender digital inclusion

The first step in testing mediation is to analyze the relationship between the three variables involved. In this case, a correlation analysis of relevant local content, attitude and gender digital inclusion was conducted as seen in Table 3 below.

Table 3: Correlation of relevant local content, attitude and gender digital inclusion

		RLC	Attitude	GDI
Relevant local content	Pearson Correlation	1		
Attitude	Pearson Correlation	.822**	1	
Gender digital inclusion	Pearson Correlation	.807**	.863**	1
***. Correlation is significant at the 0.01 level (2-tailed).*				

Correlation results in Table 3 reveal that there is a significant relationship between relevant local content and attitude (r=.822**, P<.05). There is also a significant relationship between attitude and gender digital inclusion (r=.863**, P<.05). Further, there is a significant relationship between relevant local content and gender digital inclusion (r=807, P<.05). According to Baron and Kenny (1986), once three relationships are significant, a regression analysis is conducted on the independent and the mediator variables. Table 4 below shows step two of Baron and Kenny procedure.

Table 4: Regressing attitude on relevant local content

Model Summary					
Model		R	R Square	Adjusted R Square	Std. Error of the Estimate
dimension0	1	.822[a]	0.675	0.674	0.55075
a. Predictors: (Constant), Relevant local content					

ANOVA[b]						
Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	199.857	1	199.857	658.886	.000[a]
	Residual	96.154	317	0.303		
	Total	296.011	318			
a. Predictors: (Constant), Relevant local content						
b. Dependent Variable: Attitude						

Coefficients									
Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	Correlations		
		B	Std. Error	Beta			Zero-order	Partial	Part
1	(Constant)	0.71	0.111		6.415	0			
	Relevant local content	0.871	0.034	0.822	25.669	0	0.822	0.822	0.822
a. Dependent Variable: Attitude									

Results in Table 4 above show that relevant local content explains 67.4% of variance in attitude (Beta=0.822, Sig=.000, R^2=0.675 and Adjusted R^2=0.674, Sig=.000). The next and last step of Baron and Kenny is to run a regression analysis of the independent, mediator and dependent variables as presented in Table 5.

Table 5: Regressing gender digital inclusion on relevant local content and attitude

Model Summary

Model		R	R Square	Adjusted R Square	Std. Error of the Estimate
dimension0	1	.880[a]	0.775	0.773	0.42345

a. Predictors: (Constant), Relevant local content, Attitude

ANOVA[b]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	194.821	2	97.41	543.263	.000[a]
	Residual	56.661	316	0.179		
	Total	251.481	318			

a. Predictors: (Constant), Relevant local content, Attitude

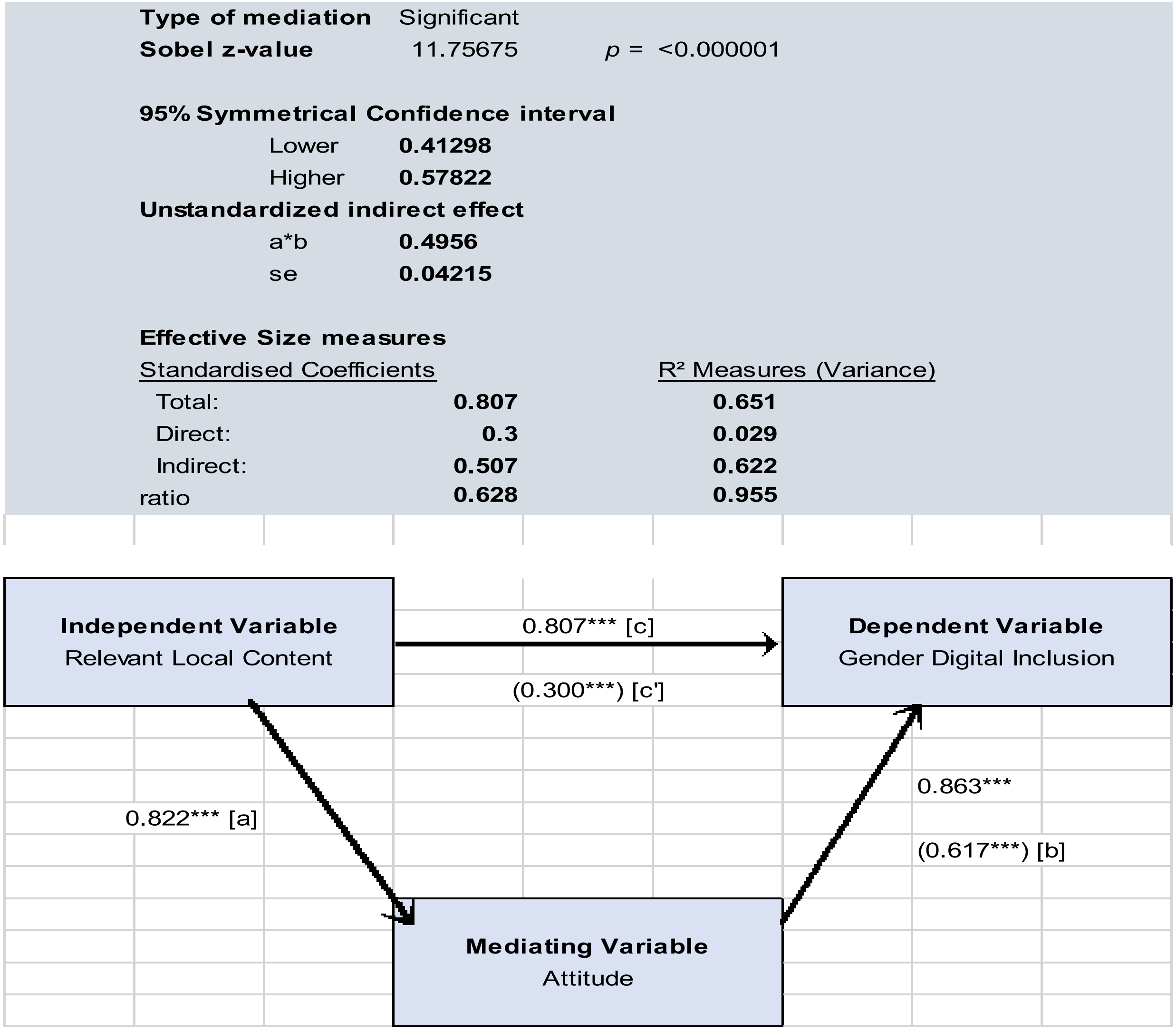
b. Dependent Variable: Gender digital inclusion

Coefficients

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	Correlations		
		B	Std. Error	Beta			Zero-order	Partial	Part
1	(Constant)	0.356	0.091		3.935	0			
	Attitude	0.569	0.043	0.617	13.175	0	0.863	0.595	0.352
	Relevant local content	0.293	0.046	0.3	6.395	0	0.807	0.338	0.171

a. Dependent Variable: Gender digital inclusion

Regression results Table 5 show that relevant local content and attitude significantly predict gender digital inclusion (Beat=0.617, and 0.3 respectively, R^2=0.775, Adjusted R^2=0.773, Sig=.000). according to Baron and Kenny (1986) procedure, we can conclude at this point that attitude positively mediates the relationship between relevant local content and gender digital inclusion. However, in order to establish the mediation effects as well as pictorially present the mediation effect of attitude in the relationship between social influence and gender digital inclusion, a MedGraph by Jose (2013) was run as seen in figure 2.



```
Type of mediation      Significant
Sobel z-value           11.75675         p =  <0.000001

95% Symmetrical Confidence interval
              Lower     0.41298
              Higher    0.57822
Unstandardized indirect effect
              a*b       0.4956
              se        0.04215

Effective Size measures
Standardised Coefficients                R² Measures (Variance)
  Total:                      0.807               0.651
  Direct:                       0.3               0.029
  Indirect:                   0.507               0.622
ratio                         0.628               0.955
```

Figure 2: MedGraph of attitude mediating relevant local content and gender digital inclusion

Results in figure 2 show that attitude significantly mediates the relationship between relevant local content and gender digital inclusion (Sobel z-value= 11.75675, P<0.000001). Direct mediation effect is 2.9% (Direct R^2= 0.0290), while the indirect mediation effect is 62.2% (Indirect R^2=0.622). Total variance explained by explained by both relevant local content and attitude is 65.1% (Total R^2=0.651). These findings reveal that hypothesis H1 which states that attitude mediates the relationship between relevant local content and gender digital inclusion in Uganda was supported.

Discussion of findings

Findings revealed that Attitude mediates the relationship between relevant local content and gender digital inclusion in Uganda, thereby supporting H1. This finding is in agreement with literature which argues that women have a negative attitude towards ICT and therefore tend to like and use computer less (Colley and Comber, 2003), feel less comfortable with computers (Cooper and Weaver 2003) and are less likely to enjoy and feel less involved with computers than men do (Mucherah, 2003). Women actually perceive that their abilities are significantly lower than men's (Cooper, 2006; Correa, 2010; Hargittai & Shafer, 2006), which eventually may affect their motivation towards using digital technologies. Such negative attitudes discourage women from being included in the digital world thus widening the gender digital gap. It is noted that the biggest challenge for women participating in the digital sector is that digital content is often not tailored to women and thus leave out topics of interest to them.

A report by ITU (2017) explains that a number of women who are not connected to the internet feel that they will gain little value from internet access or content, while others do not make more extensive use of the internet due to the lack of relevant content tailored to women. Thus, efforts need to be put in place to improve on the Attitudes of women towards using digital technologies. This can be done by inducing women's effectiveness/ feelings toward digital technologies, sensitizing women on the usefulness of digital technologies, eliminating difficulties women face when using digital technologies which can lead to perceived control of women when using digital technologies.

Conclusion and recommendations

H1 stated that Attitude positively mediates the relationship between relevant local content and gender digital inclusion in Uganda. The findings from correlation, regression and MedGraph analyses revealed that indeed attitude positively mediated the relationship between relevant local content and gender digital inclusion in Uganda. Hence, this study concludes that attitude positively mediated the relationship between relevant local content and gender digital inclusion. Therefore, in order to achieve improved gender digital inclusion, efforts should be made to improve on women's attitudes towards using digital media as it has been found to be a significant mediator. Efforts also need to be made on adding relevant local content which is affordable and available especially for women both in urban and rural areas of Uganda. This can be done by inducing women's affectiveness/ feelings toward digital technologies, sensitizing women on the usefulness of digital technologies, involving women in creating digital content, using local languages in creating relevant digital content, eliminating difficulties women face when using digital technologies which can lead to perceived control of women when using digital technologies

Limitations of the study and Future work

This study was conducted mainly on women who were relatively educated. As seen in the demographic statistics, the lowest education level of respondents was O' Level, which is reasonably good education. Thus, the respondents were not illiterates. Aware that many women in Uganda are illiterates, without having even completed primary level education, and that they cannot read and write, it is possible that the findings of this study may not universally apply to all categories of women including the illiterates. Given the above limitation, we suggest that a study on gender digital inclusion of uneducated women in Uganda be conducted.

References

Ajzen, I., & Fishbein, M. (2005). The influence of attitudes on behavior. *The handbook of attitudes*, *173*(221), 31.

Abdullah, Z. D., Ziden, A. B. A., Aman, R. B. C., & Mustafa, K. I. (2015). Students' attitudes towards information technology and the relationship with their academic achievement. *Contemporary Educational Technology*, *6* (4).

Antonio, A & Tuffley, D (2014).The Gender Digital Divide in Developing Countries. *Future Internet 2014, 6 (*4*)*

Bourdieu, P (1984) Distinction: A Social Critique of the judgment of Taste, MA *Harvard University Press*

Coleman, J (1990). Foundations of Social Theory. Cambridge: *Harvard University Press*.

Cooper, J. (2006) The Digital Divide: The Special Case of Gender. Journal of Computer Assisted Learning 22(5)

Correa, T. (2010). The participation divide among "online experts": Experience, skills, and psychological factors as predictors of college students' web content creation. *Journal of Computer-Mediated Communication*,16(1).

Colley, A. & Comber, C. (2003). Age and Gender Differences in Computer Use and Attitudes among Secondary School Students: What Has Changed? *Educational Research, 45*(2).

Cunningham, C. (2007). Linking STEM and Communication Technology Research: A Research Agenda for Technology and Gender Equality Paper presented at the annual meeting of the NCA 93rd Annual Convention, TBA, Chicago, IL.

Davaki, K. (2018). The underlying causes of the digital gender gap and possible solutions for enhanced digital inclusion of women and girls. *European Union.*

Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1989). "User Acceptance of Computer Technology: A Comparison of Two Theoretical Models," *Management Science, 35* (8),

Davis, F. (1986). *A* technology acceptance model for empirically testing new end-user information systems: theory and results. *Unpublished doctoral dissertation, Massachusetts Institute of Technology.*

Fishbein, M., & Ajzen, I. (1975) Belief, Attitude, Intention and Behavior: An Introduction to Theory and Research, *Addison-Wesley, Reading, MA*.

Global System for Mobile Communication Association (2015). Mobile phones, internet, and gender in Myanmar. London: GSMA. Retrieved on 12/10/2018 from: https://www.gsma.com/mobilefordevelopment/

Global System for Mobile Communication Association (2015 a). Accelerating Digital Literacy: Empowering women to use the mobile internet. Retrieved on 03/03/2019 from: https://www.gsma.com/

Hafkin, N and Taggart, N (2001). Gender, Information Technology, and Developing Countries: An Analytic Study

Helsper EJ and Eynon R (2013) Distinct skill pathways to digital engagement. *European Journal of Communication,* 28(6).

International Center for Research on Women (ICRW) (2012). Connectivity: How mobile phones, computers and the internet can catalyse women's entrepreneurship.

ITU (2017). ITU Facts & Figures. Geneva: ITU. Retrieved on 18/10/2018 from: http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2017.pdf

ITU (2016). ITU Facts & Figures. Geneva: ITU. Retrieved on 18/10/2018 from: http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2016.pdf

Jope, A. (2017). Gender equality is 170 years away. We cannot wait that long. *World Economic Forum.*

Krejcie and Morgan (1970). Determining sample size for research activities. *Educational and Psychological Measurement*

Lekhanya*,* L. M. (2013). Cultural Influence on The Diffusion and Adoption of Social Media Technologies by Entrepreneurs in Rural South. *International Business & Economics Research Journal (IBER)*, *12* (12).

Lin, N (2000). Inequality in Social Capital. Contemporary Sociology, *American Sociological Association,* 29 (6).

Melhem, S., Morell, C. and Tandon, N., (2009). Information and communication technologies for women's socio-economic empowerment. *The World Bank.*

Meraz, S. (2008). Women and technology: How socialization created a gender gap. *New York: Routledge*

Microsoft, UNESCO, UN Women & ITU (2014). Girls in STEM and ICT Careers: The Path toward Gender Equality. Retrieved on 12/12/2018 from: http://www2.tku.edu.tw/

Moghaddam, G., G. (2010). Information technology and gender gap: toward a global view. *The Electronic Library, 28 (5).*

Mucherah, W (2003) The Influence of Technology on the Classroom Climate of Social Studies Classrooms: A Multidimensional Approach. Learning Environments Research

National Information Technology Authority [NITA] Survey2017/18 Report. Retrieved on 10th / 11/2018, *https://www.nita.go.ug/sites/*

Organization for Economic, Co-operation and Development [OECD], (2018). Bridging the Digital Gender Divide; Include, Upskill, Innovate.

Patil, D.A., Dhere, A. M & Pawar, C. B (2009) ICT and empowerment of rural and deprived women in Asia. *Asia-Pacific Journal of Rural Development*.

Pinch, T., & Bijker, W. (1987). The social construction of facts and artefacts: Or how the sociology of science and the sociology of technology might benefit each other. *Social Studies of Science,14*(3)

Rhema, A., & Miliszewska, I. (2014). Analysis of student attitudes towards e-learning: The case of engineering students in Libya. *Issues in Informing Science and Information Technology, 11.*

Roscoe, J. (1975). *Fundamental Research Statistics for the Behavioural Sciences.* New York: Holt Rinehart & Winston.

Sandys, E., 2005. Gender equality and empowerment of women through ICT. *Women 2000 and beyond*.

Saunders, M., Lewis, P., & Thornhill, A. (2009). *Research Methods For Business Students (*4thed.). London: Prentice Hall.

Selwyn, N. (1997). Students' attitudes toward computers: Validation of a computer attitude scale for 16-19 education. *Computers & Education*, *28*.

Spante, M., Hashemi, S. S., Lundin, M., & Algers, A. (2018). Digital competence and digital literacy in higher education research: Systematic review of concept use. *Cogent Education*, *5*(1).

Tulinayo, F. P., Ssentume, P., & Najjuma, R. (2018). Digital technologies in resource constrained higher institutions of learning: a study on students' acceptance and usability. *International Journal of Educational Technology in Higher Education*, *15*(1).

UNESCO (2013). Global Media and Information Literacy Assessment Framework: Country Readiness and Competencies, Paris: UNESCO

Van Deursen, A., Van Dijk, J., Peters, O. (2012). Proposing a Survey Instrument for Measuring Operational, Formal, Information and Strategic Internet Skills. *International Journal of Human-Computer Interaction, 28*(12).

Velnampy, T., (2008), "Job Attitude and Employee Performance of Public Sector Organizations in Jaffna District, Sri Lanka", *GITAM Journal of Management*,.*6*(2).

Varank , I. (2007). Effectiveness of Quantitative Skills, Qualitative Skills, And Gender In Determining Computer Skills and Attitudes: A Causal Analysis. *A Journal Of Educational Strategies, Issues and Ideas*, *81* (2).

Uganda Bureau of Statistic [UBOS] (2014). National Population and Housing Census 2014.

Zhao, Y (2013) The Gender Digital Divide. Unpublished Master thesis, Lund University

Zher, S.Y & Chye, C.S (2017) Developing a digital literacy scale & measuring digital diusingPIAAC data. 4thPIAAC International Conference S

About the Authors

Michael Koyola

Michael Koyola has a keen interest in Digital inclusion.

Bonface Abima

Bonfacr Sbima is a lecturer at Makerere University Business School, Faculty of Computing and Informatics in the Department of Computing Science an d Engineering with a research interest in digital inclusion, e-services, and educational data mining and learning analytics.

Geoffrey Mayoka Kituyl

Geoffrey Mayoka Kituyl is a senior lecturer at Makerere University Business School, Faculty of Computing and Informatics in the Department of Computer Science and Engineering with a research interest in digital inclusion, social media usage, e-health and e-learning.

Robert Kyeyune

Robert Kyeyune is a senior lecturer at Makerere University Business School, Faculty of Computing and Informatics in the Department of Applied Computing and Information Technology with a research interest digital inclusion and ICT4D.

Bernard Engotoit

Bernard Engotoit is a lecturer at Makerere University Business School, Faculty of Computing and Informatics in the Department of Computer Science and Engineering with a research interest in digital inclusion, e-agriculture adoption and e-health technologies usability.

Changing Training to Improve On-the-Job Cybersecurity Performance

Dr. Jane LeClair Washington Center for Cybersecurity Research & Development

Dr. Tanis Stewart Thomas Edison State University

Dr. Denise Kinsey University of Houston

Abstract

This paper encourages a change in how organizations, trainers, and trainees view training—the support provided for it, the type of training developed, the types of evaluation utilized to measure training success, as well as the need for a change in perspective on training achieved partially through self-reflection and new methods of analysis in order to achieve the required performance on the job to reduce cyber incidents.

Introduction

Cybersecurity remains as one of the top concerns facing businesses today. By some estimates, cybercrime will cost the world $6 trillion annually by 2021 (Morgan, 2020). Over the years businesses have devoted a great deal of their resources to defending their digital information, investing in hardware and software and developing training programs. One area in particular is awareness training. Cybersecurity awareness training is offered in organizations for the purpose of educating employees about cybercrime. Most often organizations are complying with industry regulations or frameworks such as the Payment Card Initiative (PCI-DSS), Health Insurance Portability and Accountability Act of 1996 (HIPAA), Sarbanes-Oxley (SOX) reporting requirements, National Institute of Standards and Technology (NIST) or International Standards

Organization (ISO). Organizations are generally training employees to avoid cyber heists through phishing attacks, ransomware attacks, account takeovers, or other security breaches that threaten the organization's assets (Cybercrime Magazine, 2020). Cybercrime is moving at light speed and continues to grow in both numbers and ferocity. The FBI's Internet Crime Complaint Center (IC3) provides the public with a mechanism for reporting suspected Internet-facilitated criminal activity. It reported a total of 467,361 complaints with reported losses exceeding $3.5 billion in 2019 (FBI 2019 Internet Crime Report). Whether to comply with industry regulations or to help employees raise their understanding of potential cybercrime activities, the need for awareness training is growing.

Cyber security 'awareness' training can be developed in-house by Information Technology (IT) or Training departments but is more often provided by professional organizations that specialize in delivering products, services and platforms for employee education, phishing simulation, and related assistances (Cybercrime Magazine, 2020). These department or company trainers by definition are responsible for educating employees on a variety of topics related to identifying and guarding against cybercrimes. Some of the top providers have websites and advertisements that boast of using modern training techniques to teach employees to identify email-borne threats, how to defend against hackers, and how to protect data. Pride is taken in offering simulated phishing exercises and other security attacks (Cybercrime Magazine, 2020). However, based on the number of cyber breaches that continue to occur each year, caused in many cases, by employee failure to adhere to cyber hygiene, it appears many of these training programs have been ineffective.

Efforts have been made to improve training but limited focus has been given to include the affective domain in the design and implementation of the training. The affective domain is vital for the success of the training in transferring the lesson material back to the workplace. Affective domain objectives, a part of Bloom's and others' educational and training codifications, when applied to cybersecurity training, could create a learner commitment from lower level awareness and attitude up to promotion and value of the cyber hygiene behaviors. Organizations look for from their employees to move beyond mere awareness of cyber hygiene to promotion and valuing of the cyber behaviors so needed in today's workplace.

When we look at the 'what' that is being offered to trainees the focus is on the technical information related to the most prevalent cybercrimes as mentioned above. When we look at 'how' cyber awareness training is being offered to trainees, the methods generally focus on using asynchronous web-based training to develop a competency in trainees in identifying and preventing cybercrimes. While best efforts can be made to address 'what' is taught regarding changing cultures through affective domain objectives, a renewed interest should be placed in 'how' it is taught from the perspective of the actual trainer. Aside from the material in a book, instructors often possess a wealth of knowledge that may add to or conflict with what is in print. Schon (1983) writing of trainer's reflection back on their training notes queried: "What is the kind of knowing in which competent practitioners engage? How is professional knowing like or unlike the kinds of knowledge presented in academic textbooks, scientific papers, or learned journals?" With that in mind, trainers should reflect on the outcomes they see as a result of their packaged training and consider any alterations that might provide better results.

Trainers should consider utilizing Kirkpatrick's Four-Level Training Evaluation Model. With this model the trainer first seeks the reaction of the trainees to the lesson to determine how they felt about the session. Second, the trainer should test the skills of learners before and after the learning session to determine if learning has occurred. Third, trainers or supervisors should observe the trainees on the job after the session to determine if the skills and knowledge have been transferred to the workplace. Finally, trainers should measure results by comparing the expected outcomes against calculated and observed results to determine the return on investment (ROI). Is the cost of the training effectively changing employee behaviors in order to reduce their organizations cyber risk?

Mezirow's 'Perspective Transformation' challenges trainers to step outside of their comfort zone and reexamine how they are presenting topics. For example, trainers might consider changing their methods or teaching techniques based on their audience. Knowing your audience and getting them involved in the training is an important key to effective training. Freitfeld (2013) writes that "It is not your audience's job to be engaged or be persuaded; it is up to you to persuade them" (p. 1). While this position offers one author's view of the training 'dance' between trainer and trainee, some responsibility must assuredly rest with the learners to connect with the material in some form in order to adequately transform their 'learning' into behavior change. Learning cannot be said to take place until it is demonstrated by behavior change. Therefore if the learner gets 'checked off' as completing the training but has not learned enough to make true behavioral change, they cannot be said to have learned the material and should not receive a 'completion' merely to cover the requirement to 'receive training'. Management as well as the trainer must recognize that any time that we accept a 'completion check off' as indicating that someone has been trained, we are not only fooling ourselves but are doing a disservice to the our organizations and society at large by certifying that learning and thus behavior change has taken place when indeed we have not verified that this is true.

The Organization/Management

The type of training, how it is offered, and how it is viewed largely depends on the culture and views of the organization. Before the trainer can conduct a needs assessment of the training, a performance analysis should be conducted on the organization. This analysis has to be all encompassing by focusing on individual and organizational performance. It needs management buy-in and participation. Overall it uses a systems approach to identify performance needs and shortfalls. The goal is to identify why cybersecurity training is not producing the required results. Is it a training issue per se, is it a management issue, or a perception issue? Several questions need to be addressed such as, how does management feel about cybersecurity training? Is it management that is not allowing the trainers to develop quality training…possessing a 'just get it done' attitude? Has the needs analysis not shown a need for ownership by the audience/employees? Has management implied that this is 'get it done' training vs 'something we really care about having our employees embrace'? Is it the trainers who developed the training that have made it a 'check off' kind of slide presentation online training? Have they used any affective objectives to engage learners and help them find value from the topic/training? Using this systems approach to identify performance needs and shortfalls will provide trainers with the information needed to begin their perspective transformation.

Once the performance analysis is complete and these questions have been answered organizations can proceed by offering professional development for trainers with the goal of providing guidance on how to approach training differently. The train-the-trainer program could be based on a combination of elements from various models of transformative learning. Trainers would be shown methods that guide them through reflective thinking. They would be given assistance redesigning their programs to include the missing elements of the affective domain and given the opportunity to practice constructing affective domain objectives. They would be introduced to and shown how to use the tools and techniques described above that allow for developing new material; and assistance in developing the appropriate evaluation criteria and a practical approach for implementing the Kirkpatrick's training evaluation model. The end result of this train-the-trainer program would be a new training strategy with action plans, methods and models that were derived from critical reflective activities.

When a training initiative begins, management has already recognized that in order for a task to be completed by workers, training for that task must be undertaken. The expectations of management are that the assigned trainer will dutifully impart the necessary knowledge to the workers. The training regimen can be in a prepackaged form provided by a vendor, developed by the trainer in-house, or an already existing training package that has been modified to suit the need. Whatever the format, the training should be engaging with the trainer owning the training and with all parties buying in to the experience. Through use of affective domain objectives, the training will have a greater impact on the learning experience by ensuring that the trainees' attitudes and values are impacted—and without the full spectrum of knowledge, skills and attitudes, the learning will not be fully instilled or internalized in the learner.

The Trainers

While it is important to consider 'what' is being offered to trainees, it is also important to consider how the material is presented. The above-mentioned suggestions are some examples of what trainers might consider in rethinking how they do their job. For Perspective Transformation to occur the trainer has to become a reflective practitioner. Schon (1983) defines reflective practice as "the practice by which professionals become aware of their implicit knowledge base and learn from their experience." Merickel (1998) uses this as a basis and contends that "developing a reflective process involves asking and answering the fundamental questions of: "what do I do?; how do I do it?; and what does this mean for both myself as a professional and those whom I serve"? Perhaps the first step is for the trainer to critically examine their own assumptions and beliefs about training in order to foster an awareness of these beliefs and answer these questions (Cranton and King, 2003). Gaining an awareness of their approach to training and reflecting on the underlying reasons behind their approach will help them develop a different perspective about training (Cranton, 1996). The ultimate goal is for trainers to see themselves as change agents in the cybersecurity awareness training arena (Lysaker and Furuness, 2011).

To be a change agent and truly make a difference in how training is viewed by the organization and how it is received by the audience, a comprehensive review of what is currently taught is also a must. A good starting point for trainers is to incorporate the affective domain learning objectives into the existing technical course objectives. Affective objectives typically target the awareness and growth in attitudes, emotion, and the degree of acceptance or rejection. These objectives are classified on a five layer continuum that moves the learner from the basic step of receiving new ideas and material to responding to these ideas, to being willing to value the idea, to relating the idea to their existing values and finally reaching a characterization level where employees consistently act in accordance with the new idea (Krathwohl, et all 1964).

Including the affective domain in cybersecurity training has positive benefits for the employees and the organization as a whole. It will result in all levels of the organization having a better understanding of the need for the training. Employees will value the training and the time they spend attending it. They will view it as something more meaningful than simply ‘checking the box’. It will also reinforce positive behavior and promote the continued enforcement of cyber policies within the organization. It will promote a shift of the entire organizational culture in terms of cybersecurity training and cybersecurity culture (Kinsey, LeClair and Stewart, 2020).

Websites and training advertisements indicate that cybersecurity awareness training is accomplished by teaching the latest terminology, showing videos, and offering simulated phishing exercises and other security attacks (Cybercrime Magazine 2020). SecureWorks (2018) identifies exercises that teach employees how to recognize common hacking attempts and how to respond to spam, phishing, social engineering and other similar issues. These are good methods, but these focus on the technical aspects of the subject and fail to incorporate the affective domain objectives. Using the new lens that resulted from the perspective transformation process along with a set of learning objectives that addresses both the technical and affective aspects of cyber security awareness, trainers can revise and sometimes replace these training technique to make each more inclusive.

The goal of the revised training curricula is to develop training that teaches the technical aspects in a way that modifies the trainees’ behavior. One way to do this is to use a situational approach. Introduce the trainees to situations and preferred ways to respond through the use of video clips and multiple technologies that aid in understanding and retention of the information. Create discussion topics and techniques that allow the trainees to respond by putting themselves into the actual situation so they learn how to react as if they are on the job. Use job specific scenarios that include discussions on why a choice is correct or more correct than another in a security scenario. All these methods need to be tailored to the specific job responsibilities of the particular audience. Customizing the material for each audience makes it relevant and more impactful (Kinsey, LeClair and Stewart, 2020).

The final step is for trainers to evaluate their new approach to gain knowledge about how it is working and to pinpoint the strengths and weaknesses of the training. As previously mentioned, one tool to use is Kirkpatrick's four level model. Incorporating all four levels of the model is more difficult and time-consuming, but it provides the most valuable information. Level 1 is trainee focused and provides positive and negative comments from the trainees which can be used to modify the program. Level 2 focuses on content evaluation and provides information on what employees learned as a result of attending the training. Level 3 addresses the issue of learning transfer as it provides data on the employee's job performance as a result of applying what they learned during the training. Level 4 is when the organization attempts to measure organizational changes due to the training (Kirkpatrick & Kirkpatrick, 2005, 2006). Level 4 is believed to be the most important and the most challenging level to assess (Werner & DeSimone, 2005; Kirkpatrick, 1960; Kirkpatrick, 1998; Phillips, 1996). Because of this, trainers normally stop at Level 2. It is the authors' opinion that implementing the entire model is needed if a behavioral change is the goal. It is well worth the time and effort as it will provide a comprehensive evaluation of the effects of the training on both the individual and the organization as a whole.

The Learners

R. Eric Thomas (2020) is once quoted as saying "Who am I doing this for, and do they want what I want" (p. 10)? Trainers and educators have one perspective on a learning event, but the audience may have an entirely different view. The key to a successful event is to get both the audience and the trainer/educator to agree to the expectations of the final outcome. If both parties are not aligned, the training could very well be ineffective.

Most often when we discuss training, we are examining it from the trainer or manager viewpoint. This would include much of what has been written on the subject and often, as we have done earlier in this article, tried to help the trainer reflect on their current training scheme and assess whether they are really meeting the objectives of successful training or merely checking the box that indicated training was presented and completed.

In this section we will look at the training from an audience perspective. What is the purpose of the training? How is it presented to the audience? Is the training interesting, engaging and is the audience learning the material or merely remembering the material enough to take the test and move on with their other work? Is the audience able to take the behaviors learned in the training back to the workplace and put them into practice? If not, what is holding them back from doing this? This is also the key aspect that must be explored.

The learners must visualize the training's value in order to 'accept' and internalize the training. One of the primary ways to accomplish this, and to stop reliving the mistakes of previous, ineffective training events, is for trainees to change their perspective on how they view training. Perspective transformation, as we know, is a change in how we view things (and ourselves). As we get involved with this change we seek to become more inclusive and reject the old concepts of us and them, the all knowing trainer and the audience, and work together towards a relationship that fosters collaborative learning—an intellectual and behavioral change. As discussed the trainer must reflect inward to note what worked well in the past and what was ineffective or should be improved, rejecting lockstep methods of teaching and adopting creative methods and techniques that meet the needs of the particular audience. This leads to seeing the trainees in a new light as active participants vs passive observers to the training. So while this self-reflection is needed for the trainer, it is also necessary for the learners if they are to get the most out of the training and out of their job. While the trainer has the responsibility to set the training up to change the learning environment, the trainees must be led to self-reflect on how they approach the training and the transfer of learned skills and techniques back to the workplace if we are to see appreciable behavioral change and thus positive changes in the workplace.

Once the training is complete, it is vital for the trainer to determine if the training has been effective. As discussed with Kirkpatrick's Training Evaluation Model, it becomes clear that it is usually only the first two levels that are commonly used, and then often not fully. End-of-course evaluations, or 'smile sheets' tell us if the learners 'liked' the training. This is an important step in moving from avoidance behaviors to approach behaviors; in other words, having trainees to connect with the material and information vs avoiding the new learning and going back to old habits. However, we need to go beyond simply testing trainees at the end of the event and drill down to really determine if the training has been effective. After the trainer gauges the reaction of the audience by 'listening' to the trainees' feedback to identify if the training resonated with them, (what they did or didn't like, if they find it applicable, potential changes), the trainees should be tested in the learning level prior to the event, and then again after the training to determine what was learned, and ensure the results of the testing match the learning objectives. Key to this success is the behavior level where the trainees transfer what they have learned back to the workplace to ensure they are now applying the newly learned concepts on the job. This is where true 'learning' takes place, as learning is actually 'behavioral change', not merely test taking. Through observation by either the trainer or management on the job, they determine if the trainees have transferred their training to the workplace effectively or if they are still using the pre-training behaviors. Transference of concepts is a key measurement of success that clearly indicates the learners have internalized the learning and displayed the requisite new behaviors on the job. A change in perspective has taken place which indicates they have accepted the need for change.

A Model for Cybersecurity Consciousness Training

In order to make substantial change to employees' on-the-job cybersecurity behaviors, a reassessment to the organization's approach to cybersecurity training must take place. To this end, a model for change which includes the organization, the trainers and the learners (employees) can be implemented to facilitate a step-change in cybersecurity behaviors in the workplace. The organization, trainers and learners must move from cybersecurity awareness training to cybersecurity consciousness training. The organization must ensure that change in standards for cybersecurity training are clear to the trainer and the learner, that standards are reinforced with trainers and learners as well as front line supervision. Front line supervisors must support these changes and ensure they, through their actions, are part of this change solution. The organization must support process changes for the trainers in order to ensure time and resources are provided for implementing personnel, training, and evaluation changes that will lead to successful behavioral changes. Trainers must ensure deficiencies are identified in all areas, whether in the cognitive, psychomotor or affective dimension. The training must change the required behavior on the job. Trainers and learners must take an active part in the learning, become more self-aware of their value in achieving the organization's training goals. By reevaluating their view of the organization's commitment to cybersecurity training, they must re-evaluate their own on-the-job behaviors with regard to cybersecurity to ensure they are demonstrating strong cybersecurity behaviors on the job. All parties, the organization, the trainers and the learners/employees must have clear expectations for the needed changes and understand their role in making the organizational changes successful.

Model for Cybersecurity Consciousness Training

OWNER	ACTIONS	EXPECTATIONS
Organization	➢ Support trainer change actions ➢ Support for perspective transformation ➢ Support for performance analysis	➢ Training moves from awareness to value-based training ➢ Provide resources for trainers and learners change initiatives ➢ Performance analysis identifies missing knowledge, skills and attitudes
Trainers	➢ Embrace perspective transformation ➢ Include affective domain objectives ➢ Take time for self-reflection ➢ Expand training evaluation measures ➢ Perform performance analysis	➢ Embrace change of employee value of training is incorporated in the training ➢ Ensure affective objectives address organizational values focused on employee cyber performance ➢ Identify what you are changing and are not changing to move training to next level ➢ Move from Level 3 to Level 3 evaluation and institute transfer-of-training measures ➢ Identify specific items in training or on-the-job needed to reflect a change in job performance
Learners	➢ Become an active participant ➢ Identify the value of training ➢ Reevaluate perspective of training ➢ Embrace transfer of training to the job	➢ Identify expectations from the organization for trainers and learners ➢ Embrace organizational support for the value of cybersecurity training ➢ Raised self-awareness of behaviors both in and after training ➢ Be aware of supervisory support for transfer of training back on the job

Conclusion

As ongoing events in the world have clearly illustrated, cybersecurity training is important to all organizations seeking to protect valuable electronic date from those with nefarious intent. Hackers will continue their assaults on the data systems of organizations large and small in a relentless effort to leverage stolen information for monetary gain. Since the vast majority of cyber breaches are a result of erroneous human interaction with hackers, it behooves organizations to constantly train and retrain their employees to resist the efforts of bad actors. This can only come about with efficient cyber training that discards the ineffective training methods of the past and embraces new methods that seek to dramatically involve both trainers and learners in an experience that benefits the learners—and in the long run the organization as a whole.

We use this article as a Call to Action to organizations to support their training in a manner that will move it from required 'check-off' sessions, to a learning experience that the organization, the trainers, and the learners can take pride in to achieve the type of cybersecurity training that will make a positive difference. Organizations can clearly see that check-off training is making little difference in changing behaviors on the job. Trainers must move to performance analysis to identify the areas needed to change in order to support the new organizational standards for cybersecurity training and employee cyber behavior back in the workplace. Ownership of cybersecurity is everyone's responsibility, not merely the IT department. If we are to make the progress needed to thwart the number of successful cyber breaches, we must take the steps necessary at all levels of the organization—through management support, trainer and learner involvement to achieve our goals.

References

Cranton, P. (1996). Professional Development as Transformative Learning: New Perspectives for Teachers of Adults. San Francisco, CA: Jossey-Bass Inc.

Cranton, P. and King, K.P. (2003). Transformative Learning as a Professional Development Goal. New Directions for Adult and Continuing Education. 98: 31-37.

Cybercrime Magazine (2020). List of Security Awareness Training Companies to Watch In 2020. Retrieved from https://cybersecurityventures.com/security-awareness-training-companies/

FREIFELD, L. (2013). *7 SECRETS TO ENGAGING AN AUDIENCE*. RETRIEVED FROM HTTPS://TRAININGMAG.COM/CONTENT/7-SECRETS-ENGAGING-AUDIENCE/

Kinsey, D., LeClair, J., and Stewart, T. (2020). Culture Shift Needed in Cybersecurity Training. *Journal of Women and Minorities in Technology*. Retrieved from https://campussuite-storage.s3.amazonaws.com/prod/1280306/3a32f069-629b-11e7-99ef-124f7febbf4a/2043053/de7890b4-3eca-11ea-8279-12c513967203/file/JWMIT-V1-I2.pdf

Krathwohl, D.R., Bloom, B.S., and Masia, B.B., (1964). Taxonomy of Educational Objectives, Handbook II: Affective Domain, New York, NY. David McKay Company, Inc.

Kirkpatrick, D. L. (1998). Evaluating training programs: The four levels (2nd ed.). San Francisco, CA: Berrett- Koehler Publishers.

Kirkpatrick, D. L. (1960). Techniques for evaluating training programs: Learning. *American Society for Training and Development Journal,* 18, 28-32.

Kirkpatrick, D.L. and Kirkpatrick, J.D. (2005). Transferring learning to behavior: Using the four levels to improve performance. San Francisco, CA: Berrett-Koehler Publishers.

Lockwood, S. L. (2001). Enhancing employee development: Development and testing of a new employee orientation protocol. (Doctoral dissertation, California School of Professional Psychology. (San Diego, 2001). *Dissertation Abstract International, A62/03*,166.

Lysaker, J. and Furuness, S. (2011). Space for transformation: Relational, dialogic pedagogy. *Journal of Transformative Education*. 9 (3): 183-187. Doi:10.1177/1541344612439939 https://doi.org/10.1177%2F1541344612439939. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.1002.9078&rep=rep1&type=pdf

Merickel, M. L. (2020). Reflective Practice, The Reflective Practitioner, Oregon State University, School of Education, copyright paper, 1998. Retrieved from Oregonstate.edu/instruct/pte/module2/rp.htm

Morgan, S. **(**2020**)**. Cybercrime Damages $6 Trillion By 2020. Retrieved from the https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

Philips, J. J. (1996). ROI: The search for best practices. *Training & Development*, 50(2), 42-47.

SecureWorks (2018, Nov 12). Cybersecurity Awareness Training: Threats and Best Practices. Retrieved from https://www.secureworks.com/blog/cybersecurity-awareness-training-best-practices

Schon, D.A. (1983). The Reflective Practitioner: How Professionals Think in Action. Basic Books Inc.

Thomas, R. E. (2020). Here for It: Or, How to Save Your Soul in America; Essays. Ballantine Books.

Wertz, C. (2005). Evaluation of CLAD training in northern California. (Doctoral dissertation, University of Southern California, 2005). Dissertation Abstract International, A66/06, 108.

About the Authors

Dr. Jane LeClair

Dr. Jane LeClair is the President and CEO of the Washington Center for Cybersecurity Research & Development whose mission is to increase knowledge of the cybersecurity discipline. Before assuming her current position, Dr. LeClair was the Chief Operating Officer at the National Cybersecurity Institute (NCI) in Washington, D.C., previously served as Dean of the School of Business and Technology at Excelsior College and had a 20-year career in commercial nuclear power. Dr. LeClair has written and edited numerous books, journals and articles related to cybersecurity, nuclear technology and education and is a staunch advocate for women in technology.

Dr. Tanis Stewart

Dr. Tanis Stewart is a consultant who focuses on information technology and cybersecurity Awareness. She is fully committed to promoting women in technology and cybersecurity. Dr. Stewart has held numerous industry Information Technology positions including Network Engineer, Vice President of Network Engineering, and Director of Information Technology. She has worked as an adjunct professor and Instructional Designer at several universities in the United States, Europe and Asia.

Dr. Denise Kinsey

Dr. Denise Kinsey has consulted in IT and OT cybersecurity for many years including projects in business, manufacturing, financial, medical, nuclear, and ethanol production. Denise's academic career includes her present position as Assistant Professor at the University of Houston, a Carnegie designated Tier I Research School. She has published several books and articles in various cybersecurity topics. She is co-chair of the National Institute of Standards and Technology (NIST) National Initiative for Cybersecurity Education (NICE) curriculum project. Her relevant certifications include the CISSP, C|CISO, and Security+.

Cybersecurity Leadership Guiding the Pathway Forward

Venessa Howard, Ph.D.
Randall Sylvertooth, Ph.D

The purpose of this article is to emphasize the facts and impacts leadership has on moving forward in the progression of cybersecurity developments despite cybersecurity criminals and other cyber actors. The potential of the internet has grown over the years and the impact it has on businesses and organizations can be frightening. The key reason for this is trust in the internet and the ability of organizations to secure their assets. Over the past two decades, the internet has transformed many aspects of modern life. Building trust and confidence is one of the main enablers for the future growth and use of the internet. Law and collaboration is necessary to build the trust and safeguards that are necessary for businesses' and organizations' operations to survive and operate over the internet.

The evolving cyber-threats and potential impact has grown systematically over the years. The risk of performing business comes at a price to the business and the consumer. Further considerations from different stakeholders build on the risk and more secure information pathway and this has to be devised for existing business's critical infrastructure. The questions outline possible pathways that can take us forward with our leaders that have been given a better understanding of various cybersecurity issues and challenges that have been involved in building confidence and other cybersecurity practices.

Along with increasing of new threats to network and information security has emerged. The expansion and misuse of electronic networks, for criminal purposes pose a real threat to the security of the enterprise. The objectives of the adversary can furthermore adversely affect the integrity of critical infrastructures within states. A concrete pathway forward that can be changed and built upon with suggestions on how countries could look at the issues related to cybersecurity. Hackers and the attacks which they carry out have changed significantly over the past few years. Hackers are developing malicious code more quickly, and they are becoming more technically sophisticated in the way they circumvent network controls such as anti-virus software and firewalls. Their attacks are more advanced and targeted, affecting specific industries, internets, groups, and people. As a result of phishing, especially via botnets, businesses and consumers are adversely impacted by tremendous financial losses, identity theft, and other damages. The existence of botnets which can enable phishing and the ensuing damage, due to theft of critical personal or business information. The e-mail scams that motivate personnel to click on the malicious spam act as intermediaries to circulate malicious activity throughout the organization. Phishing email preys upon the ignorance of many users causing their fear. Warning e-mails that ensues before and after a compromise will assist the user in contacting and preforming adequate safeguards. Training and blogging on the different website about best security practices may assist the user in providing due diligence at work and at home. Increasingly sophisticated, context-aware phishing is making the phishing scams more credible.

Context-aware phishing attacks are much more successful than traditional phishing attacks (Jakobsson and Ratkiewicz, 2006)

As threats to cybersecurity are constantly evolving, cybersecurity policies and actions must be flexible and adaptive. As there are many different stakeholders involved, the government needs to determine the roles of institutions and their related responsibilities to ensure cybersecurity at the national level. Typically implementing a national strategy requires coordinating across multiple authorities and organizations in different government departments. Each department must determine the level of cybersecurity risks to which it is willing to accept and expose its citizens and organizations along with the involvement of its various agencies. As the different government departments' stakeholders bring different perspectives to the problem, one of the first tasks is to evaluate a multitude of national vulnerabilities. Utilizing statistical data to map against vulnerabilities, the agencies and other information may lead to the next agency or organization that is most likely to be breached. The responsibility of leaders to defend different government agencies and organizations needs to be productive and preventive in nature.

The speed and connectivity of new and improved technology devices that are currently used to commit malicious actions have increased, making system network enterprises even more vulnerable to cyber threats. The availability of information and the speed of information being exchanged along with the relative anonymity of online transactions have complicated many cybersecurity practices (Clarke, Richard A. & Khake, Robert K., 2019). The technical complexity, variety and inter-connectivity of system network enterprises and information database systems are all also threatened by malicious cyber activities. Therefore, cybersecurity managers must be allowed to mitigate the identified security risks where they are very much prevalent. Technology-centered mitigation countermeasures can be deemed as a promising paramount solution. However, to a large extent, modern mitigating solutions which have been adopted have had a short-sighted view of cybersecurity (Pfleeger and Caputo, 2012). Therefore, leaders will need a more predictive analytic approach and better cyber threat intelligence to assist in being more proactive rather than reactive in mitigating various cybersecurity threats in the future. The operational challenges of the future for leadership lies on the fact of providing the necessary means of providing protective, preventive and predictive measures to move forward. While preventive and protective cyber countermeasures are more in demand and are the most widely used. It is the predictive methodology that can stop most cyber threats from even occurring. Predictive analysis begins with leadership examining their existing critical infrastructure and their own network enterprise systems. Leadership would be able to accomplish this feat by implementing an efficient cyber threat intelligence operation and vulnerability research knowledge management system which would focus a great deal on research and reliable data sources. There are many vendors that can provide many of these described services for predictive cyber countermeasures using cyber threat intelligence.

The cyber threat intelligence operation can feed into The Security Operations Center (SOC) by protecting the network enterprise infrastructure of a business or organization. The SOC operations can also benefit by using malware signatures, Yara and Snort rules data for successfully blocking on-going malicious traffic that may have otherwise passed through businesses' and organizations' critical network enterprise infrastructures. Having a cyber threat intelligence and vulnerability research knowledge management operation can also prevent malicious activity in a network enterprise system by feeding known vulnerabilities into the patching cycle which is critical to any businesses' or organizations' cyber hygiene operations. If leadership gave more attention to these two services it would more likely decrease the operational monitoring of malicious traffic going through the SOC. This would already be accomplished by limiting the threats of vulnerabilities and malicious activity which has occurred elsewhere. Leadership must establish a threat intelligence and vulnerability research knowledge management operation for advanced research and industry collaboration where it is composed of cyber strategists, advanced cyber technology capabilities, academics and third-party technology vendors.

The operations would make up the leadership core of both on-going operations. The core of both could further be supported by an active cyber advisory panel or council within the established business or organization. The advisory panel or council would uniquely be focused on both operational challenges of cyber intelligence and vulnerabilities to provide a better and more preventative outlook of cybersecurity countermeasures. The two operations must have a cyber threat intelligence and vulnerability research knowledge management training area for personnel under leadership to start and progress in their analytical research operations (Clarke, Richard A. & Khake, Robert K., 2019).

The training area for cyber threat intelligence and vulnerability research knowledge management should also be based on established strategies and implemented down to the tactical levels of operational control. The cyber threat intelligence and vulnerability knowledge management centers once established should have an organization which provides on-going leadership access to the over-all operation and a smaller part of the organization where the tactical operations of research, analysis, briefings, and actionable results can occur. Leadership should have the proposed operations linked to academic institutions and government agencies and departments which should be thinking hard about leadership challenges of securing a large cybersecurity attack threat surface. This attack threat surface has now recently been announced by U.S. Cyber Command as the new Fifth (5th) Domain (Clarke, Richard A. & Khake, Robert K., 2019). Therefore, there needs to be a greater collaborative research network in cyber intelligence operations not only in the military but also in business and other organizational operations. It is needed to increase the over-all capabilities of leadership to be able to continue protecting business and organizational cyber and technology assets in the 5th domain (Clarke, Richard A. & Khake, Robert K., 2019). This will allow for quicker identification of critical needs of leadership within various businesses and other such organizations. Cyber threat intelligence and vulnerability research knowledge management operations will also need active leadership for testing and experimentation operations.

The testing and experimentation can be implemented by businesses and organizations participating in cyber threat tabletop exercises. These are usually conducted by U.S. Government agencies and departments on a continuous basis (Clarke, Richard A. & Khake, Robert K., 2019). This is where leadership can use certain limited threat intelligence and vulnerability alerts in a controlled simulated real world setting to test both their strategic and tactical cyber controls for immediate incident response operations.

There is one large cyber exercise such as this to test leadership response to a cyber incident. The U.S. Department of Homeland Security's (DHS) Cyber and Infrastructure Security Agency (CISA) conducts such an exercise called Cyber Storm. Cyber Storm is going into its 7th iteration of simulated operations. Although, the development of such an organization can provide a means of having better coordinated cybersecurity incident response and countermeasures, threatening cybersecurity issues will still remain and are far from being contained and resolved by today's methods of cyber threat operations.

Finally, once leadership has been able to establish, build, collaborate, learn and test their capabilities, they must be able to sustain the new focus of the described operations (Clarke, Richard A. & Khake, Robert K., 2019). The importance of sustainment of such operations is for identifying new challenges within the operational environment and to implement new opportunities coming from academic institutions and global technology companies. Therefore, in this case, the proposed operations of a combined threat intelligence center and a fully functional vulnerability research knowledge management center integrated with SOC operations will be needed to increase the capability of predictive cyber threats. However, these operations will still require extensive needs and a considerable amount of work to improve cyber operations in businesses and organizations. Leadership must definitely be very prevalent as a stakeholder in this ongoing cyber operations endeavor to be effective.

References

Jakobsson, M. and Ratkiewicz, J. (2006), “Designing ethical phishing experiments: a study of (ROT13) rOn”, Indiana University, Bloomington, IN, available at: www2006.org/programme/files/pdf/3533.pdf.

Noble, H. and Smith, J. (2015), “Issues of validity and reliability in qualitative research”, Evidence-Based Nursing, Vol. 18 No. 2, pp. 34-35, BMJ Publishing Group Ltd and RCN Publishing Company.

Noluxolo Gcaza, Rossouw von Solms, Marthie M. Grobler, Joey Jansen van Vuuren, (2017) "A general morphological analysis: delineating a cyber-security culture", Information & Computer Security, Vol. 25 Issue: 3, pp.259-278, https://doi.org/10.1108/ICS-12-2015-0046

Pfleeger, S.L. and Caputo, D.D. (2012), “Leveraging behavioral science to mitigate cyber security risk”, Computers & Security, Vol. 31, Elsevier Ltd, pp. 597-611.

Sund, C. (2007) "Towards an international road-map for cybersecurity", Online Information Review, Vol. 31 Issue: 5, pp.566-582, https://doi.org/10.1108/14684520710832306

Clarke, Richard A. & Khake, Robert K. (2019). The Fifth Domain; Defending our Country, Our Companies and Ourselves in The Age of Cyber Threats. New York, NY; Penguin Press

About the Authors
Venessa Howard, Ph.D.

Dr. Howard has over 30 years’ experience in Security Management, Information Technology, including the management of Enterprise Architecture, Systems Analysis, Policy and Planning, Application Software, Network Services, IT Security, Data Management and Customer Support. She has provided expert technical advice and guidance to federal agencies, private citizens affected by malicious software, scams, and Internet hoaxes. She has a doctorate in Management with a concentration on Homeland Security.

Randall Sylvertooth, Ph.D

Dr. Randall Sylvertooth is a well-seasoned technology subject matter expert who has worked for multiple U.S. Government Defense Contractors improving the security of critical infrastructure, physical security and cybersecurity for U.S. Federal Agencies and Departments. He has a B.S. in Architecture and Urban Design Planning, a M.S. in Information Systems, a M.S. in Cybersecurity, and a D.Sc. in cybersecurity.

AI Data Privacy and Bias: Issues to be Managed

Charles Parker, II, Ph.D.

Abstract

Machine learning and artificial intelligence continues to increase its processing power. This has been possible due to improved technology and the amount of data available increasing exponentially. The improved processing is useful for analysis and to predict future behavior. While this is a benefit, there are issues associated with this. Namely consumer privacy and bias. While pertinent, advancing the usefulness of these have been highlighted more than the consumer's effects. There are inherent issues which may be encountered with this due to the data, methods of collection, and other aspects. These are explored along with ramifications from not addressing these.

Data has been present since the dawn of time. As civilization advanced, so did the methods of capturing data. With the improved means of recording with advanced machines and equipment, the amount of recorded data expanded exponentially. This mountain of data is created every single day. The estimates of the volume vary. By 2025, approximately 463 exabytes (EB) will be created every 24 hours. These are certainly impressive amounts of data. One of the significant contributors to this are the connected and autonomous vehicles (CAV). Each connected vehicle collects data not only from the vehicle's internal operations, but also the operators and passenger's interactions with the vehicle. The connected aspect and sensors for the CAV provides the mass amount of data required for the system to operate (Bagloee, Tavana, Asadi, & Oliver, 2016). This data includes information on the location of other vehicles, air flow interacting with the engine, traffic data, and roadway conditions, to name a few examples (Montanaro, Dixit, Fallah, Dianati, Stevens, Oxtoby, & Mouzakitis, 2018). The vehicle also collects traffic signal data, speed limit, vector, speed acceleration, steering angle, brake status, and vehicle size (Folk, 2016). For the CAV, Gartner estimates these will create 280 petabytes (PB) of data per year beginning in 2020 (Engineering.com, 2019; Hines, 2016). Autonomous vehicles are still in development with significant advances. The autonomous test vehicles create 5 TB -20 TB of data for every day of testing, dependent on the type and number of sensors per vehicle (Mellor, 2020).

The amount of data collected in the present and future will not decrease. The automakers continue to add more advanced sensors and equipment to the vehicles, which increases the amount of data being collected. As the amount of data increases, the need for analysis grows in amount and complexity. The amount and different types of data provide the opportunity to analyze connections, correlations, trends, and other data-related aspects. Data analysis is far beyond the simple spreadsheets of a decade ago. The amount of data is simply too large. There are statistical applications available to work with this volume.

Business and scientists are using more artificial intelligence (AI) to not only analyze the data, but also to predict behavior. AI in this application learns from the system's experiences. The system uses the experiences and data sets to solve problems it is presented with (Datatisynet, 2018). The present usage of AI includes machine learning (ML) in its learning process. Another aspect of this includes the AI system making decisions without input from outside sources based on the experience and data set analysis (Meyer, 2018; Kim & Mejia, 2020). Examples of these are Amazon, Google, Facebook, Uber, and Lyft (Kim & Mejia, 2020). The technology allowing the AI viability are primarily due to the large data sets and improvements in processing power and GPUs (Lipton, 2019).

The data collected from the vehicles represents a person's life and experiences. These data sets hold the individual's personally identifiable information (PII) (e.g. the person's phone contacts, text messages, GPS locations, and emails (ClearMyCarData, 2019)). This data describes the person's activities and could be used to create a profile. This, regardless of the end usage, is the person's private data and should have the ability to decide how and if this is used.

While the data provides a vast improvement and allows for more visibility into the operations, bias continues to be an issue. This may originate from the code or data as it is used by the AI system. While the programmers intend to code in a fair and independent manner, their respective bias may present itself with the output. The data itself, based on the creation and collection methods and other factors may also create the issue. These two factors affecting data usage and the persons (privacy and bias), have sparked many issues and debates. These will continue to do so.

Prior Research

Creating a standard to remove the inherent bias from algorithms is a focus of the IEEE P7003 working group (Koene, Dowthwaite, & Seth, 2018). The intent is to apply ethics to autonomous and intelligent systems. The deliverable would be a protocol to detect and mitigate the "unintended, unjustified, and/or inappropriate biases" (Koene, Dowthwaite, & Seth, 2018, p. 39). Previously the preponderance of AI research has been with the Trolley Dilemma. This classical ethical question involves a trolley going off of its tracks and would hit and kill innocent humans. The question is who should the trolley hit? Bonnefron, Shariff, and Rohwan (2015) addressed this. Their research indicted using the utilitarian algorithm may actually increase the autonomous vehicle (AV) casualties.

This was also addressed by Etzioni and Etzioni (2017). The AI incorporated equipment and machines will require the capability to make the difficult ethical decisions. The researchers noted there may not be a point to attempt to teach the AI modules in vehicles ethics since humans have been attempting this for hundreds of years without a clear direction. Etzioni and Etzioni (2016) previously analyzed this from the AV vehicles instruments. At this point, the research indicated the vehicle's AI system may be best suited to have an AI oversight system. This would function to monitor and audit the AI sub-system.

AI ethics is a large field. To narrow, and organize this, a taxonomy was suggested (Yu, Shen, Miao, Leung, Lesser, & Yang, 2018). The research indicated this should be divided into researching the ethical dilemmas, creating frameworks for the individual ethical decisions, having a collective framework, and human-AI ethical dealings.

While data has value, there has been a gap with comprehending the extent this may increase the productivity and efficiency of AV (Montanaro, Dixit, Fallah, Dianati, Stevens, Oxtoby, & Mouzakitis, 2017). The research indicated the vehicle's connectivity has a benefit for performance and as indirectly improvise the industry as the number of connected vehicles increases.

Bagloee, Tavana, Asadi, and Oliver (2016) conducted a literature review focused on a variety of issues associated with AV development. Their research indicated a knowledge gap with routing methods. With the data and technology available, these vehicles have the opportunity to be part of the intelligent routing system. The researchers, based on this, created a new optimized system for routing the AV.

Bensal and Kockelman (2018) analyzed the AV environment from a different view. The researchers scrutinized if society was prepared to accept the CAV on the highway environment. The research indicated, from their sample in Texas, people are prepared to pay additional fees for CAVs. Also, the respondents focus for the AD vehicles was on affordability of the features and equipment failure.

Value of Vehicle Data

For data to have a value, intrinsic or extrinsic, usefulness is required. Collecting data and storing this to the server or AWS site simply to perform the act is moot and wasteful. With vehicle data, there is a clear value to several parties. This is due to the nature of the data itself, the third-parties seeking this, and the different segments the data may be divided into for each third party's needs. The data itself, has proven to be three times as financially lucrative compared to automobile production (Fleutiaux, 2018). This symbiotic relationship has and will continue to be beneficial.

Overall, the vehicle data market is estimated to be worth $750B by 2030 (Peters, 2019). Within the next decade, this market will prove to be a driving financial force as the CAV continues their domination in the vehicle environment. As indicated, this is a massive market and provides for growth opportunities. As an example, the data may be sold. This is not a new concept or nuance on the business model. Data has been monetized by other industries in years past and increase revenues and shareholder value (Hood, Hoda, & Robinson, 2019). This is a strong driving force to gather a greater level of data and advance the AI system. The target markets are varied per the data usage. For example, the OEMs may use this to improve their product (e.g. when parts are likely to fail, and inventory becoming more efficient), urban planners and advertisers for location based analytics, insurance companies (e.g. data on speed, acceleration, and navigation), and developers to create new ideas for products and services (Peters, 2019). Each of these parties has their specific data sets and uses. These are viable clients for the data indefinitely.

The collected vehicle data may be described as per the collection method. This may be labelled as Administrative and Sensor-Related data. The Administrative Data is not from the vehicle operating, however, is generated from the different operations and activities. This begins with design, advances to development and production, sales, maintenance, and repairs (Fleutiaux, 2018). The Sensor-Related Data originates from the vehicle's sensors as these function while the vehicle is operating. This includes the cameras (may be engineered to gauge where the driver is looking (Naqvi, Arsalan, Batchuluun, Soon, & Park, 2016)), or nearly vehicles (Qin, & Wang, 2017), LiDAR and RADAR to create a data map of the surroundings, and other sensors in the proof-of-concept (PoC) stages prior to being implemented. The sensors also collect geolocation, vehicle performance, and driver behavior data. (Hood, Hoda, & Robinson, 2019) In addition to the data having an inherent value, AI adds to this by analyzing the data and creates insights from the activity (Inside Big Data, 2019). This new information, as compared to the basic data, allows the data owner to leverage this into new business, and creates another saleable, revenue producing stream.

The information is also used for the AI to drive decisions based on their algorithms (IEEE, n.d.). These decisions impact vehicle performance and safety. Due to the potential impacts there has to be an environment of trust (Marshall, 2019).

AI Data Privacy

Collecting massive amounts of data is not new. For decades this has been completed for the various work groups in the automobile and other industries. The marketing, advertising, and other departments have fully benefited from the data nada dancing technologies effect on this. In this case, ML analyzes the data to create inferences (MacCarthy, 2019) and decisions (Lord, 2020).

At the academic level, the Institutional Review Board (IRB) is formed to ensure humans aren't harmed by the research. In the vehicle field, we don't have this in place. The best tools available are statutes, e.g. GDPR in the EU, and the CCPA in California (Datatilsynet, 2018). There are also laws in place to address discrimination. These both, however, do not directly address the AI privacy and bias issue, and applying these to AI uses cases is difficult at best. These should be updated to address AI governance.

Data and Information

AI takes massive amounts of data and analyzes these for patterns. The patterns create insights. (Meyer, 2018) With the AI systems, and the products of their analysis, there is the distinct potential in harming, directly or indirectly, humans or vulnerable groups (MacCarthy, 2019). These have a value for industry for their products and future decisions. This is used in most industries at varying levels, including electrical utilities (Bartholomew, 2016), genetic testing (Hendricks-Sturrup, & Lu, 2019), and medical records (Price II, & Cohen, 2019).

Privacy

Privacy in this use case involves the human's data at rest, in transit, and when it is modified (Deane, 2018). This is no different than in the vehicle environment. There may be the consumer's data stored in the module, the data may be amended, and may be transmitted to servers or AWS sites.

Data privacy continues to be a serious issue (Lohr, 2019). One of the issues involves anonymity. The vehicle owners and operators have a right to privacy. With the data collection methods, there are certain markers indicating where the data was generated. There are methods to anonymize the data to sanitize these markers which generally work well. AI has the processing power to de-anonymize the data. AI has the processing ability to couple this data with other sources (e.g. blogs, social media, and third parties) to create a profile for each person. The AI system may also apply predictive analysis to create decision models based on the data (Meyer, 2018). With the vehicle applications, the AI system would be able to use the sanitized or non-sanitized data in the same way. The trend analysis would show the operator's driving patterns, where the person probably works, easts frequently, and other trends to predict their future behavior.

This is possible due to AI's integral functions. This is centered with AI's speed, scale, and automation (Deane, 2018). The speed addresses the system's ability to compile and analyze by far faster than any human. The additional features with this is the processing may also be increased by simply adding hardware. The scale factor also is pertinent. AI is able, without the comparative maximized effort, to analyze mass amounts of data in an exceptionally timely manner. Lastly, the AI is automated and performs the assigned tasks without external input. While this is timely, the analysis is also efficient While focusing on these shows the benefits, the issues with data privacy are a significant concern.

The other significant issue with AI implementation as it relates to humans is bias. Seemingly, there should not be a bias with AI as this processing the program's code. Bias may creep into the process through two main sources-data and training.

The algorithms themselves may be biased based on the training data (Datatilsynet, 2018; Challen, Denny, Pitt, Gompels, Edwards, Tsaneva-Atanasova, 2019; Robins, 2020). While the intent may be to have clean data, this may not be the case due to sampling bias, survey not vetted to the appropriate extent, and other factors. There may also be an issue with the algorithm's learning process. While the program may be coded to be fair and balanced, the learning process may skew the results. There are many examples of this in recent years. There have been issues with the sentiment-analysis of sentences, recidivism assessment models, and facial recognition software. (Menzies, 2020) Other examples directly affecting humans occurred when Microsoft's chatbot learned to be racist form its data set (i.e. humans interacting with the chatbot), and Los Angeles police department using predictive algorithms with questionable results (Leong, 2019). This bias may be inadvertently applied to vehicle data and operations through the analysis and usage.

Discussion

Data, and especially data from the CAV, needs to be fair and accurately represent the usage, persons, and circumstances. The ML/AI applications need to be applied without bias

(Menzies, 2020; Lord, 2020). Skewing this, intentionally or not, has direct and potentially serious applications.

The training data and learning algorithms used by AI systems have to use fair, balanced data without bias and misuse. The potential for issues vary with the automobile application. The automobile owners may be the victim of data exploitation. The owners often are not aware of how much data their vehicle actually creates, analyzes, and shares. The data may be used to identify specific persons, track them, and monitor the vehicle's and accessory usage. While sanitizing the data may be attempted, the AI system has the capability to reverse this process.

The AI systems use data for predictive purposes. The users future driving patterns may be estimated by the system. While this seems mundane, this may be used as a detriment to the person. The output form the AI could be purchased, or a third-party could purchase the data and process this with their own algorithms, to predict the user's driving behaviors, their future location, and use this to adjust their billing for insurance or future vehicle purchases or other malicious purposes.

Profiling is a rather significant issue. While this may be used for analysis, this may also be used for scoring, classifying, and evaluating people. As this data is analyzed, the profiling is based on historical data. This does not take into account their present circumstances or updated behaviors since the last data collection. This has the potential to negatively impact people until the data is re-evaluated, whenever that may be. This is commonly done without the consent of the person's affected. The vehicle created data which could be used by third parties.

The privacy and bias AI issues bring the potential to harm those in vulnerable groups. These persons don't have the ability to adequately address this. There are laws in place confronting discrimination. These were written years and decades ago prior to AI being prevalent and used to the extent it is.

At this point in the industry, there needs to be additional research focused on engineering AI systems to comply on a greater level with the regulations and spirit of these. The first step is to apply the research to more pronounced guidance. The vehicle's data, which should be without bias, may be used in manners not consistent with the programmer's intent.

The updated governance should update the transparency, allowing others to know what data is collected, allowing the users to opt out, and detailing the purpose and uses of the collected data (Forbes Insights, 2019).

References

Bagloee, S.A., Tavana, M., Asadi, M., & Oliver, T. (2016). Autonomous vehicles: Challenges, opportunities, and future implications for transportation policies. *Journal of Modern Transportation, 24*(4), 284-303. Doi:10.1007/540534-016-0117-3

Bartholemew, A. (2016). The smart grid in Massachusetts: A proposal for a consumer data privacy policy. *Boston College Environmental Affairs Law Review, 43*(1), 79-110.

Bensal, P., & Kockelman, K.M. (2018). Are we ready to embrace connected and self-driving vehicles? A case study of Texans. *Transportation, 45*(2), 641-675. Doi:10.1007/s11116-016-9745-z

Bonnefon, J. (Shariff, A., & Rahwan, I. (2016). The social dilemma of autonomous vehicles. *Science, 352*(6293), 1573-1576. Doi:10.1126/science.aaf2654

Challen, R., Denny, J., Pitt, M., Gompels, L., Edwards, T., & Tsaneva-Atanasova, K. (2019). Artificial intelligence, bias, and clinical safety. *BMJ Quality Safety, 28*(3), 231-237. Doi:10.1136/bmjqs-2018-008370

ClearMyCarData. (2019, April 30). How is your personal data put at risk by your car? Retrieved from https://www.clearmycardata.com/blog/how-is-your-personal-data-put-at-risk-by-your-car

Datatilsynet. (2018, January). Artificial intelligence and privacy. Retrieved from https://www.datatilsynet.no

Deane, M. (2018, January). AI and the future of privacy. Retrieved from https://towardsdatascience.com/ai-and-the-future-of-privacy-3d5f6552a7c4

Desjardins, J. (2019, April 17). How much data is generated each day? Retrieved from https://www.weforum.org/agenda/2019/09/how-much-data-is-generated-each-day-cf4bddf29f/

Engineering.com. (2018, August 8). Making connected vehicles generates 10x data as driving them. Retrieved from https://www.engineering.com/AdvancedManufacturing/ArticleID/19442/Making-Connected-Vehicles-Generates-10X-Data-as-Driving-Them.aspx

Etzioni, a., & Etzioni, O. (2016). AI assisted ethics. *Ethics and Information Technology, 18*, 149-156. Doi:10.1007/510676-106-9400-6

Etzopmo. A., & Etzioni, O. (2017). Incorporating ethics into artificial intelligence. *The Journal of Ethics, 21*(4), 403-418. Doi:10.1107/s10892-017-9252-2

Fleutiaux, F. (2018, February 27). Vehicle data is more profitable than the car itself. Retrieved from https://www.telekom.com/en/company/management-unplugged/francois-fleutiaux/details/vehicle-data-is-more-profitable-than-the-car-itself-516208

Folk, E. (2016). Fundamental privacy concepts for connected vehicle deployments. Retrieved from https://www.its.dot.gov/pilots/pdf/CVP_TechAssistWebinar_Privacy_v4.pdf

Forbes Insights. (2019, March 27). Rethinking privacy for the AI era. Retrieved from https://www.forbes.com/sites/insights-intelai/2019/03/#33a0d70d7f0a

Hendricks-sturrup, R.M., & Lu, C.Y. (2019). Direct-to-consumer genetic testing data privacy: Key concerns and recommendations based on consumer perspectives. *Journal of Personalized Medicine, 9*(2). Doi:10.3390/jpm9020025

Hines, J.F. (2016, September 7). Forecast: Connected car production, worldwide. Retrieved from https://www.gartner.com/en/documents/3436517

Hood, J., Hoda, O., & Robinson, R. (2019, January 4). Monetizing data in the age of connected vehicles. Retrieved from https://www2.deloitte.com/us/en/insights/industry/automotive/monetizing-data-connected-vehicles.html

IEEE. (n.d.). AI is driving AVs, but whose ethics are driving AI? Retrieved from https://innovationatwork.ieee.org/ai-is-driving-avs-but-whose-ethics-are-driving-ai/

Inside Big Data. (2019, December 17). Yes, data privacy and artificial intelligence are compatible. Retrieved from https://insidebigdata.com/2019/12/17/yes-data-privacy-and-artificial-intelligence-are-compatible/

Kim, T.W., & Mejia, S. 92010, February). From artificial intelligence to artificial wisdom: What Socrates teaches us. *Computing Edge*, 8-12. Doi:10.1109/MC.2019.2929723

Koene, A., Dowthwaite, L., & Seth, S. (2018). IEEE P7003 standard for algorithmic bias considerations. 2018 ACM/IEEE International Workshop on software Fairness. Doi:10.1145/3194770.3194773

Leong, B. (2019, February 20). Artificial intelligence: Privacy promise or peril? Retrieved from https://fpf.org/2019/02/02/artificial-intelliegnece-privacy-promise-or-peril/

Lipton, B. (2019, November 19). The U.S. needs to "get AI right"-and fast-says government group. Retrieved from https://www.muckrock.com/news/archives/2019/nov/19/national-security-commission-on-ai-report/

Lohr, S. (2019, April 3). A.I. and privacy concerns get white house to embrace global cooperation. Retrieved from https://www.nytimes.com/2019/04/03/technology/artificial-intelligence-privacy-oecd.html

Lord, J. (2020, February 3). Artificial intelligence will require oversight, regulation. *Crain's Detroit Business, 36*(5), 8.

MacCarthy, M. (2019, April 1). How to address new privacy issues raised by artificial intelligence and machine learning. Retrieved from https://www.brookings.edu/blog/techtank/2019/04/01/how-to-address-new-privacy-issues-raised-by-artificial-intelligence-and-machine-learning/

Marshall, K. (2019, February). Autonomous vehicles: The AI and ethics challenge. Retrieved from https://home.kpmg.au/en/home/insights/2019/02/trust-autonomous-vehicles-ai-ethics-challenge.html

Mellor, C. (2020, January 17). Data storage estimates for intelligent vehicles vary widely. Retrieved from https://blocksandfiles.com/2020/01/17/connected-car-data-storage-estimates-vary-widely/

Menzies, T. (ed.) (2020, February). Think your artificial intelligence software is fair? Think again. *Computing Edge*, 14-18. Doi:10.1109/MS.2019/2908514

Meyer, S. (2018, December 26). Artificial intelligence and the privacy challenge. Retrieved from https://www.copmagazine.com/data-privacy/artificial-intelligence-and-the-privacy-challenge/

Montanaro, U., Dixit, S., Fallah, S., Dianati, M., Stevens, A., Oxtoby, D., & Mouzakitis, A. (2018). Towards connected autonomous driving: Review of use cases. *Vehicle System Dynamics, 57*(6), 779-814. Doi:10.1080/00423114.2018.1492142

Naqvi, r.A., Arsalan, M., Batchuluun, G., Yoon, H.S., & Park, K.R. (2018). Deep learning-based gaze detection system for automobile drivers using a NIR camera sensor. Sensors, 18(2), 456. Doi:10.3390/s18020456

Peters, J. (2019, May 23). Automakers have a clear choice: Become data companies or become irrelevant. Retrieved from https://techcrunch.com/2019/05/23/automakers-faced-with-a-choice-become-data-companies-or-become-irrelevant/

Price II, W.N., & Cohen, I.G. (2019). Privacy in the age of big data. *Nature of Medicine, 25*(1), 37-43. Doi:10.1038/s41591-018-0272-7

Qin, L., & Wang, T. (2017). Design and research of automobile anti-collision warning system based on monocular vision sensor with license plate cooperative target. *Multimedia Tools and Applications, 76*(13), 14815-14828. Doi:10.1007/511042-016-4042-6

Robbins, S. (2020). AT and the path to envelopment: Knowledge as a first step towards the responsible regulation and use of AI-powered issues. *AI & Society, 35*(2), 391-400. Doi:10.1007/s00146-1019-00891-1

Vuleta, B. (2020, January 30). How much data is created every day? Retrieved from https://seedscientific.com/how-much-data-is-created-every-day/

Yu, H., Shen, Z., Miao, C., Leung, C., Lesser, V.R., & Yang, Q. (2018). Building ethics into artificial intelligence. arXiv preprint arXiv:1812.02953 (2018).

About the Author

Charles Parker II, PhD

Charles Parker has over a decade of experience in the InfoSec industry beginning in the banking industry and continuing through the medical and vehicle industries. He focused on improving InfoSec environment through presenting on various subjects, writing extensively on cybersecurity Application and breaches and consulting. His current research projects are focused on vehicle, maritime, and satellite attacks, along with AI and quantum computing. Charles currently works at Stephenson Technology Corporation as a Senior Information Systems Security Engineer.