Barun ICT Global News

July 2022

YONSEI UNIVERSITY Barun ICT Research Center

01

NFTs: Changing the World of Dance

Fountine ZHAO

Department of International Studies/Drama, UC Irvine

In our ever-changing and expanding era of digitalization, technological innovation is creating new opportunities in different artistic fields. NFTs are currently rising in popularity in producing unique pieces of digital media of dance pieces, opening new doors for dancers to flourish.

The pandemic has been difficult for dancers and their industry. As live performers, the limitations on face-to-face interactions made it difficult to earn income. However, the creation of dance NFTs allows dancers to sell their iconic moves and earn big bucks from them, especially in the booming gaming industry.

Street dancer Cjaiilon Andrade, also known as Snap Boogie, founded a company called Beauty in the Streets (BITS) that works with the blockchain platform Enjin, to enable performing artists and dancers to develop NFT-based "emotes" or animated emojis. People can buy tokens to use the NFT to perform dance moves in AlterVerse, which is a 3D PC and VR game [1].

Three TikTok dancers - Jalaiah Harmon (the creator of Renegade), Cookie Kawaii (the creator of Throw it back), Blanco Brown (the creator of The Git Up)— partnered up with La Canda-based AR production house

Jada and Culver City-based studio partner Metastage, to create NFT holograms of themselves performing their iconic dance moves. They were sold at an auction on NFT marketplace Open Sea, and the holograms are available for use on the app Jadu. This allows users to interact with holograms of celebrities and creates videos to share on social media. The topic of proper compensation and giving proper credit to dancers has been controversial. On TikTok, black creators were especially struggling. However, by monetizing their moves through NFTs, creators can retain an ongoing stake in a digital asset, receiving percentages of any sales they make [2].

In addition to the collaboration of trendy dance moves and the gaming industry, there are other types of NFTs made by dancers of various styles. According to Euronews, Russian ballerina and principal dancer for London's Royal Ballet, Natalia Osipova, created the first ballet NFT, sold at the auction "Encore! Modern Art on Stage" starting at £12,000 and £50,000 for her two pieces [3]. Reported by Dance Magazine, dancer and physicist Mariel Petee created a program allowing her to create performances of AI-generated choreography in response to her dancing body [4], opening up another possibility for dancers to make money digitally. Tap dancer Savion Glover is selling an NFT video of himself discussing his creative process in a package that also includes a physical signed commemorative print [4].

Although similar types of media are available for free on the Internet, people are still willing to pay for the right to claim ownership of things associated with famous dancers. As of now, NFTs are not practical enough for dancers in general to make money, as those who create dance NFTs at the moment were already internationally famous enough to start their items at high prices. However, as the metaverse continues to develop and expand, NFTs have increasing potential to provide opportunities to all dancers.

Sources

[1] Sinclair, S. (2021, March 16). Performers' dance moves turned into animated nfts for games and apps. CoinDesk Latest Headlines RSS. Retrieved May 31, 2022. https://www.coindesk.com/markets/2021/03/16/performers-dance-moves-turned-into-animated-nfts-for-games-and-apps/

[2] Blake, S. (2022, May 26). This startup is using NFTs to give black dance artists credit for their creations. dot.LA. Retrieved May 31, 2022. https://dot.la/tiktok-dance-nfts-jadu-2653455538.html

[3] Gallagher, T. (2021, November 29). World's first NFT Ballet set to go on sale. Euronews. Retrieved May 31, 2022. https://www.euronews.com/culture/2021/11/29/dancing-to-a-new-tune-world-s-first-nft-ballet-set-to-go-on-sale

[4] Skybetter, S. (2022, April 8). The Unlikely Pairing of NFTs and Dance. Dance Magazine. Retrieved May 31, 2022. https://www.dancemagazine.com/nfts-and-dance/

02

The Future of Cybersecurity in the Context of the US-South Korea Digital Alliance

Georgia ROBERTS

Department of Political Science and International Relations, UIC, Yonsei University

At the end of May, President Joe Biden met with the newly inaugurated South Korean President Yoon Suk-yeol for their first summit. As formally released by the White House, the two discussed how the US and South Korean alliance can improve in cyber security with an emphasis on moderating attacks made by the DPRK [1]. South Korea's position and advancement within the ICT field allows for its cyber space to be prone to threats and breaches of security [2].

Within the first half of 2021, it was reported that South Korea faced more than 127 cyber-attacks - double the amount recorded in 2018 and 2019 [3]. The DPRK has been the suspected culprit, with the most commonly known attacks being on Sony Pictures Entertainment and the Korea Hydro and Nuclear Power Company. The DPRK were blamed for both, however the actions taken by the two administrations were opposite. The Department of Justice of the United States in 2018 indicted a North Korean programmer hired by the DPRK's intelligence service for the breach on Sony Pictures [4]. The attack on the KHNP power plants, which oversaw almost a third of South Korea's energy [5], was reportedly left unattended by the South Korean government and no further action was taken as noted by So Jeong Kim, and Sunha Bae in Korean Policies of Cybersecurity and Data Resilience [6].

However, after the breach of the KHNP in 2019, the South Korean government implemented strategies in order to minimize and reduce the risk. They established the National Cybersecurity Strategy and planned to proceed with two guidelines: the National Cybersecurity Basic Plan and the National Cybersecurity Implementation Plan [7]. This not only improves cybersecurity but allows for action to be taken against aggressors. We can further see the response taken by the South Korean government through the alliance of the US and the White House press release, which stated that they hope to “broaden cooperation, on critical and emerging technologies, and cyber security [1]” it also stated that the US and South Korean governments will deepen their collaboration in areas such as cyber policy, information sharing, and military-to-military cyber cooperation, with an emphasis on other prominent international security issues [1].

With the implementation of the 2019 National Cybersecurity Strategy and the collaboration with the US to further improve joint cybersecurity measures, South Korea’s ability to deal with future cyber threats will be strengthened and improved in the years to come.

Sources

[1] The White House. (2022, May 21). United States-Republic of Korea Leaders’ Joint Statement. https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/21/united-states-republic-of-korea-leaders-joint-statement/

[2] Seok-Hoon Hong (2019). A discussion of cybersecurity from the perspective of international politics and response strategies at the national level. National Security and Strategy Institute, 19(2), 37- 75.
https://www.kci.go.kr/kciportal/landing/article.kci?arti_id=ART002477823

[3] Yonhap. (2021, July 6). S. Korea faces increasing ransomware attacks this year. The Korea Herald. http://www.koreaherald.com/view.php?ud=20210706000765

[4] Balsamo, M. & Tucker, E. (2018, Sep 6). North Korean programmer charged in Sony hack, WannaCry attack. PBS News Hour. https://www.pbs.org/newshour/nation/north-korean-programmer-charged-in-sony-hack-wannacry-attack

[5] McCurry, J. (2014, Dec 23). South Korean nuclear operator hacked amid cyber-attack fears. The Guardian.
https://www.theguardian.com/world/2014/dec/22/south-korea-nuclear-power-cyber-attack-hack

[6] Kim, S. J. & Bae, S. (2017, Aug 17). Korean Policies of Cybersecurity and Data Resilience. In E.A. Feigenbaum & M.R. Nelson. The Korean Way with Data. Carnegie. https://carnegieendowment.org/2021/08/17/korean-policies-of-cybersecurity-and-data-resilience-pub-85164

[7] Cheong Wa Dae - National Security Office. (2019, April). National Cybersecurity Strategy. https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/National%20Cybersecurity%20Strategy_South%20Korea.pdf

03

The Move Toward Green Cryptocurrency

Sereimony SEK

Department of Computer Science, Yonsei University

The 2008 Global Financial Crisis resulted in people losing trust in banks and enhanced governmental controls in regulating payments. It was also when the biggest cryptocurrency – Bitcoin - was created. During the COVID-19 pandemic, it reached its all-time of almost $69,000 in November 2020. This acceleration of cryptocurrency's value and exposure to the mainstream media comes with consequences, one of which is its environmental impacts.

Cryptocurrencies are created through a highly electricity-consuming process that requires high-tech computers with ASIC systems called mining. Mining uses a mechanism called Proof-of-Work (PoW) where many computers are needed to solve complex mathematical problems simultaneously to verify transactions [1]. As more computers are utilized in this process, more energy is consumed, resulting in a larger carbon footprint. In fact, Bitcoin mining uses 116.96 terawatt-hours (TWh) of electricity each year [2], more than some countries' entire energy usage, causing blackouts in several countries.

To prevent escalation, many researchers have been working on Green Cryptocurrency - an eco-friendly alternative with renewable energy as the most obvious approach. In 2021, it was estimated that only about 40% of Bitcoins validated by PoW were mined via renewable energy sources. Hydropower and other options are used by mining firms and individuals in Norway, though this is only feasible since Norway's electricity is entirely produced from renewable sources. While this may not be viable in all countries, we hope to see the disparity narrowing within the next years [3].

Another technique to make cryptocurrency more environmentally friendly is to use the Proof of Stake (PoS) method, which was presented by two developers in 2012. This approach uses less energy than Proof of Work because all miners do not have to be online to verify transactions. In this case, miners must deposit a modest amount of Bitcoin in exchange for a lottery-style assignment of transactions to verify. This allows them to concentrate on one problem at a time and reduce the number of processing units required [1].

Other alternatives are pre-mining and carbon credits. In pre-mining, a central authority creates a set amount of cryptocurrencies and distributes them. Transactions are still validated by a decentralized network of miners, but users may have to pay a fee. In the case of using carbon credits for cryptocurrency, mining companies have to buy the credits from others, thereby assisting in the reduction of world emissions, or converting to greener energy in order to sell their own credits [3].

Currently, there are many digital currencies such as Chia (XCH), Cardano (ADA), Nano (NANO), Stellar Lumens (XLM), and Algorand (ALGO) that are moving towards being environmentally friendly. Additionally, Ethereum proposes to use a Proof-of-Stake (PoS) consensus mechanism to reduce its energy consumption by 99.5 percent [3]. Just like any other industry, it is extremely challenging for the cryptocurrency space to reduce its carbon emissions. However, if the crypto community is willing to overcome these challenges, there is a greater potential for it to become greener. Therefore, education on green digital currencies is critical and cryptocurrency's environmental impact should not be overlooked.

Sources

[1] Gerardo, B. (2022, January 22). Is cryptocurrency bad for the environment? Fair Planet. https://www.fairplanet.org/story/is-cryptocurrency-bad-for-the-environment

[2] Cambridge Center for Alternative Finance. (n.d). Cambridge bitcoin electricity consumption Index. Retrieved May 29, 2022. https://ccaf.io/cbeci/index

[3] Iberdrola. (n.d). What are green cryptocurrencies and why are they important? Retrieved May 29, 2022. https://www.iberdrola.com/sustainability/green-cryptocurrencies

04

The Future of Charging Electronics

Jiri HAVEL

Department of Economics (MA Candidate), Yonsei University

In April 2022, members of the European Parliament voted in support of legislation that would force consumer electronics manufacturers to ensure that their new devices have a USB-C port [1]. This would, EU-wide, require all manufacturers of small devices such as phones, laptops, and speakers, that sell their products in the EU to have a functioning USB-C charging port. The main driver is the EU's commitment to reduce electronic waste by allowing customers to re-use their old chargers when buying a new device regardless of the manufacturer and type.

Although well intentioned, this legislation is behind the market trends as big players such as Samsung or Huawei already design their new devices with USB-C ports [2]. Even other smaller manufacturers of electronic devices benefit from the wide use of a universal port as they can cut costs by not including a charge. Customers can also save money and the environment when buying a new phone or headphones. This move is already happening due to market forces; hence the legislation seems unnecessary.

There is, however, one big manufacturer that does not follow the market trends: Apple. All their products have its copyrighted Lightning Connector. In effect, one may speculate that the regulation is solely targeted at Apple. Although the company has removed the charger from all new iPhone models in 2020, customers still need to purchase a new one if they switch from iPhone to another brand.

By having its own charger and data connector, Apple has the freedom to innovate. New technologies can be used to improve the port to communicate better with other devices or to be more efficient in charging the battery. This is an advantage that other manufacturers like Samsung gave up in a trade-off for cutting manufacturing costs and giving their customers the comfort to use the widely available USB-C [3].

Since the EU market is one of the largest customers for Apple, the company may face a dilemma whether to manufacture two types of devices - one with USB-C port for the European market and the other with their Lighting Connector for the rest of the world - or whether to entirely drop their connector in favor of the USB-C. Both options will certainly incur huge cost to the company, thus we may expect a legal fight between Apple and the EU on the matter. Additionally, loyal customers of Apple will be forced to change all their chargers which is contradictory to what the legislation aims to achieve.

Sources

[1] European Parliament. (2022). Common charger: MEPs agree on proposal to reduce electronic waste. https://www.europarl.europa.eu/news/en/press-room/20220412IPR27115/common-charger-meps-agree-on-proposal-to-reduce-electronic-waste

[2] Cristina Criddle. (2021). EU rules to force USB-C chargers for all phones. Protocol. https://www.bbc.com/news/technology-58665809

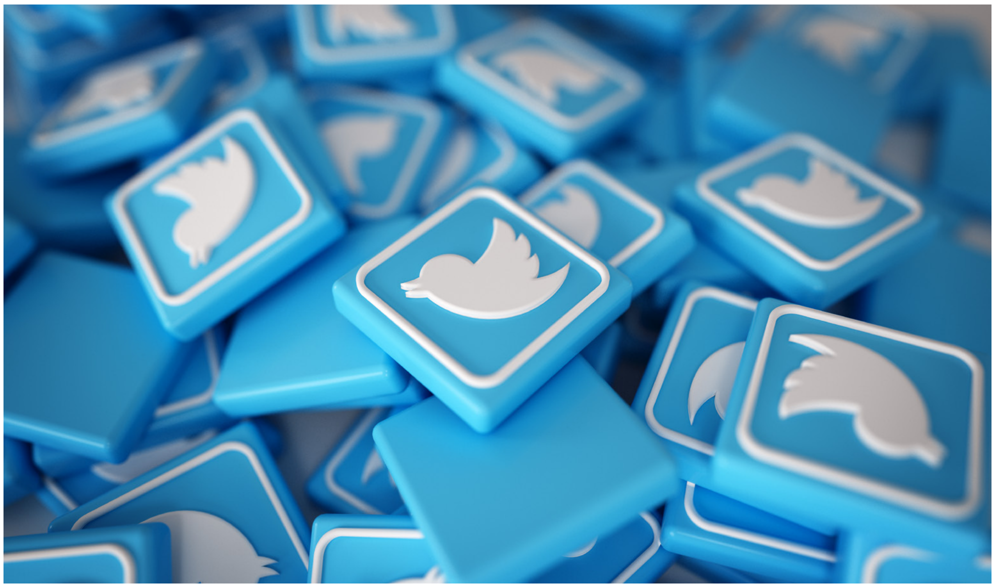
[3] Foo Yun Chee. (2022). EU deal on single mobile charging port by year end is possible, lawmaker says. https://www.reuters.com/technology/eu-deal-single-mobile-charging-port-by-year-end-is-possible-lawmaker-says-2022-02-15/

05

What Is Happening to Musk’s Twitter Acquisition?

Miriam LIM

Department of International Business, University of California, San Diego



On April 25th, Elon Musk agreed to purchase Twitter for $44 billion [1]. The agreement was set up quickly and Musk was determined to make it with little negotiation. Twitter had agreed to sell at $54.20 per share as per his request [1]. However, the deal is at a standstill; on May 14th, Musk violated Twitter’s NDA regarding information he exposed regarding Twitter’s sample size for detecting spam users and bots. He was not satisfied with the data, and tweeted, “Twitter deal temporarily on hold pending details supporting calculation that spam/fake accounts do indeed represent less than 5% of users” Following up the next day he tweeter, “Twitter Legal just called to complain that I violated their NDA by revealing the bot check sample size is 100! This actually happened.” On May 17th he tweeted “20% fake/spam accounts, while 4 times what Twitter claims, could be *much* higher. My offer was based on Twitter’s SEC filings being accurate. Yesterday, Twitter’s CEO publicly refused to show proof of <5%. This deal cannot move forward until he does [2].”

Erik Gordon, a professor of business at the University of Michigan criticized the billionaire for his lack of due diligence stating, “if the bot figure is so important to his assessment of the value of the company, he should have done his due diligence on it before signing the deal, and he should have added an explicit representation about bots to the contract [2].” The deal is on hold, and Elon continues to try and negotiate the price down. The current share price of Twitter is $38.57 in contrast to the $54.20 per share Elon agreed to purchase the company at. Conversations of Twitter suing Musk are ongoing, as well as an SEC investigation into Musk for market manipulation [3].

Originally, the deal arose due to the billionaire's interest in a perceived need for less regulation and censorship on the site. Musk is a self-proclaimed "Free speech absolutist" who was not satisfied with the site's censorship and decided to take matters into his own hands and acquire the app for himself. As an avid Twitter user with 93.8 million followers, he has moved financial mountains utilizing the app. The microblogging site has allowed the billionaire to influence cryptocurrency and Tesla Stock through tweeting a few mere words. There is speculation that his acquisition of the app will become a large source of power for his business endeavors [4].

So what are the potential dangers of this acquisition? Some of the repercussions include undoing years of hard work on the platform to protect users from dangerous content. This includes its efforts to keep hate speech, violence, dangerous activity, self-harm, and inappropriate content from minors off its site. Another is that some workers have threatened to leave the company. Workers fear that Twitter will become like Elon's companies such as Tesla Inc and SpaceX that are known for their toxic work culture; high stress with extreme working hours. As the news continues to unfold, the deal continues to become more complex as tensions between the parties increase.

Sources

[1] Gordon, N. (2022, May 23). Musk says Twitter's bot numbers are 'very suspicious'. Fortune. Retrieved May 25, 2022. https://fortune.com/2022/05/23/elon-musk-twitter-deal-bots-lower-price-renegotiate/#:~:text=On%20Saturday%2C%20Musk%20agreed%20with,of%20Twitter%20users%20were%20fake.

[2] Hirsch, L., Conger, K., & Satariano, A. (2022, May 17). Elon Musk says Twitter deal 'cannot move forward' without more information. The New York Times. Retrieved May 25, 2022. https://www.nytimes.com/2022/05/17/business/elon-musk-twitter.html

[3] Investing.com. (2022, May 27). SEC scrutinizes Musk's initial Twitter share purchases by investing.com. Investing.com. Retrieved May 30, 2022. https://www.investing.com/news/stock-market-news/sec-scrutinizes-musks-initial-twitter-share-purchases-2831105

[4] Kleinman, Z. (2022, April 25). Twitter: Why Elon Musk has been so keen on taking control. BBC News. Retrieved May 25, 2022. https://www.bbc.com/news/technology-61222793

[5] Lerman, R. (2022, May 13). Here's what Elon Musk has said about his plans for Twitter. The Washington Post. Retrieved May 25, 2022. https://www.washingtonpost.com/technology/2022/05/10/elon-musk-twitter-plans/

[6] Meierhans, J. (2022, May 11). Elon Musk would reverse Donald Trump's Twitter Ban. BBC News. Retrieved May 25, 2022. https://www.bbc.com/news/business-61399483

[7] Person. (2022, May 10). Investors think unlikely Musk buys Twitter at agreed $44 BLN price. Reuters. Retrieved May 25, 2022. https://www.reuters.com/technology/investors-think-unlikely-musk-buys-twitter-agreed-44-bln-price-2022-05-10/

06

Is Online Voting the Future?

Yewon CHOI

Department of Economics, UIC, Yonsei University

It has been almost five years since the people of South Korea expelled an incumbent president from office. Since then, the nation has gone through two more federal elections: one right after the candlelight movement of 2016 and one in May. Unfortunately however, the sense of community Koreans displayed during the candlelight vigil was not long lived. As the country went through the following elections, ideological divides worsened and social distrust increased.

One of the big issues after both was electoral fraud. The range of accusations was wide—from careless ballot handling procedures to swapping out and forged ballots, rumors of all kinds spread like wildfire [1][2]. For the earlier election specifically, the topic was debated fiercely among citizens, and almost 40,000 videos could be found online with the key word “electoral fraud” [2]. Although claims of election manipulation are not mainstream, they still maintain a level of interest. In response people began to ask if the system could be improved. Could we perhaps digitalize it? After all, most of the suspicion of the results was surrounding the management or whereabouts of physical ballots. Perhaps then the key to this problem would be to make and use a trackable digital ballot.

While the idea may sound preposterous to some, this is already happening around the world. One reason to favor online voting is that it is undoubtedly the most convenient method. Because there is no need to wait in queues just to cast a vote that may or may not directly affect the results, it can help boost turnout. Estonia is the one nation that freely allows its people to vote online for all sorts of elections [3]. France is among the few that partially provides this option to those that live abroad. The online option "had been suspended for the last legislative elections in 2017" for fears of cyberattacks, but is now back on track as of this year [4].

However, the system is not without its flaws. As with any digital system, hacking is the big problem. As more and more of our world enters the digital sphere, our money is constantly under threat of being robbed. Do we really want to take the same risks with our politics? There's already loads of evidence pointing to the fact that we do not have technology that is reliable enough to digitalize the voting process. For instance, in an event at the 2017 Def Con hacker conference, hackers tried to breach four types of voting machines. The result was that they were able to find "vulnerabilities in all four" [5]. Russia's hacking attempts in the 2016 U.S. presidential elections provide yet another reason for keeping politics separate from technology.

Barbara Simon, a former computer scientist at IBM noted that "the problem with cybersecurity is that you have to protect against everything, but your opponent only has to find one vulnerability [5]." You can always protect a piece of paper by locking it up in a room. But with electronic ballots? The vulnerabilities are endless.

Sources

[1] Ko, J. (2022, Mar 10). Irregularities continue to fan electoral fraud accusations. The Korea Herald. http://www.koreaherald.com/view.php?ud=20220310000001

[2] Song, Y. (2019, Nov 4). [Weekly fact check] "The 19th presidential election is a fraudulent election" that is still floating around. Newstof. http://www.newstof.com/news/articleView.html?idxno=2173

[3] Dimsdale, C. (2022, May 5). Can I vote online in the UK elections? Where digital voting is allowed and why you can't do it local elections. iNews. https://inews.co.uk/news/can-i-vote-online-in-uk-elections-where-digital-voting-allowed-and-why-you-cant-in-britain-1610213

[4] McNicoll, T. (2022, May 27). Mapped: Expats kick off French legislative elections with online voting. France 24. https://www.france24.com/en/france/20220527-mapped-expats-kick-off-french-legislative-elections-with-online-voting

[5] Leovy, J. (2017, Dec). The Computer Scientist Who Prefers Paper. The Atlantic. https://www.theatlantic.com/magazine/archive/2017/12/guardian-of-the-vote/544155/

07

Targeted Ransomware: How Would Your Computer Recover?

Christina LIU

Department of International Business, University of California, San Diego

With developed nations such as the United States now relying more heavily on specific software to run their daily activities on a national level, ransomware attacks have become an important cybersecurity threat due to the possibility for nefarious actors to profit from them. A case that caused worldwide mayhem was the 2017 WannaCry cyberattack that targeted computers running the Microsoft Windows operating system [1]. Starting in Asia it quickly infected over 230,000 computers in over 150 countries before finally coming to a stop 4 days later by recovering keys used to encrypt users' data [2].

Prevention is key in keeping computers safe as shown in the WannaCry attack where computers without Microsoft's security update were ultimately affected by the attack [2]. This case paved the way for more preventative measures to be implemented in order to avoid having a compromised system. Some preventative measures that have been recommended included:

1. Always having the latest antivirus update [2]
2. Keeping Windows Firewall on and configured at all times [2]
3. Typing out web addresses in the search bar [2]
4. Filtering EXEs in emails [2]

The point of these threat vectors are usually based on location and functionality of the target itself with many preferring the edge gateway due to the ease of access [3]. By getting in through this route, the attacker can then gain control over a large part of the whole system, causing more instability than just a hacking attack [3]. Edge gateways hold valuable data from "functionalities in working with critical infrastructure" to the "settings of connected devices and configuration files" making ransomware a high risk situation given the circumstance of the data becoming exfiltrated or tampered with within the cloud itself. This results in the denial of service for physical systems but also a change in the overall functionality [3]. Ransomware actors can also consider other factors when determining their target and while edge gateways have become the most common, the value of a device for an organization's productivity is also heavily considered as actors often want to compare the amount of damage it will cause in comparison to what it compromises [3].

IoT has enabled connectivity to be as fluid as possible but with it comes many vulnerabilities and actions that need to be taken in order to not compromise existing systems or data. It is also with the IoT that has allowed threat actors to be attracted to ransomware due "their vital roles and functionalities in working with critical infrastructure [3]." With these things in mind it can be easily seen why the likelihood of these attacks are so high and with so many attractive targets from physical devices to cloud servers, the most critical point of failure from the users' point of view is the fact that targets like edge gateways provide a bridge between physical and cyber worlds, a gray area between trusted and non-trusted spaces [3].

Sources

[1] Mohurle, S., & Patil, M. (2017). A brief study of wannacry threat: Ransomware attack 2017. International Journal of Advanced Research in Computer Science, 8(5), 1938-1940.

[2] Volz, Dustin (2017, May 17). "Cyber attack eases, hacking group threatens to sell code". Reuters. Archived from the original on 21 May 2017. https://www.reuters.com/article/us-cyber-attack-idUSKCN18B0AC

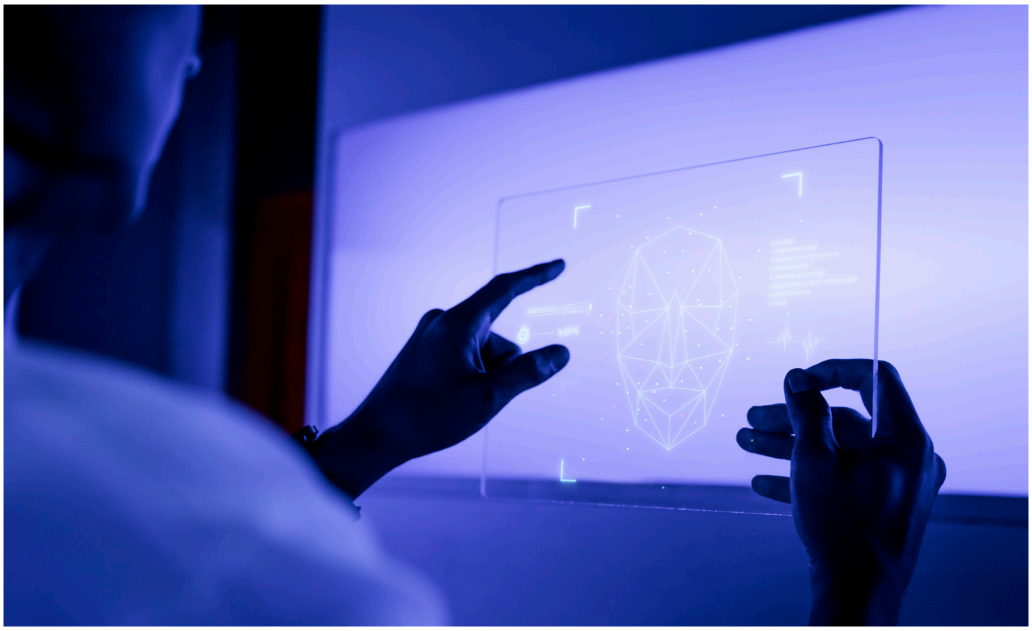
[3] Al-Hawawreh, M., den Hartog, F., & Sitnikova, E. (2019). Targeted ransomware: A new cyber threat to edge system of brownfield industrial Internet of Things. IEEE Internet of Things Journal, 6(4), 7137-7151.

08

Deepfakes: Exploring Negative and Positive Outcomes

Silva Santiago AUGUSTO

Department of Human Environmental Sciences, Yonsei University



Artificial intelligence (AI) allows for the mass production of “deepfakes”: synthetic videos that closely mimic real ones [1]. These media-synthesizing technologies are improving and becoming more affordable and user-friendly. Users can make audio or video of anyone, doing anything. For example, it is possible to use a transcript to reproduce a specific person’s voice, copy and paste one person’s face to another body, or generate completely new footage of someone speaking based on prior audio [2]. The options are limitless. This rapid advancement in the creation of deepfakes raises concerns because methods to discover misinformation induced by such technologies have yet to be disseminated.

The key risk is that deepfakes can readily lead to the formation of erroneous beliefs. Viewers may mistake deepfakes for genuine footage and assume that what they represent actually happened. Deepfakes can only prevent people from forming real beliefs if there is no alternative reputable source for the same information. However, in many cases, there is no viable substitute to video evidence that is similarly reliable. Direct visual experience provides unquestionably solid proof that an event has occurred. However, people can only make such assessments on occurrences that are physically close to them [3].

In a new report, the European Union Agency for Police Cooperation noted that deepfakes will be widely used in organized crime operations. The recent advance in AI is showing that deepfake detection and prevention must be a top priority for legal applications [4]. Generative deep learning algorithms have advanced to the point where distinguishing between what is real and fake is challenging. In the 2018 United States presidential elections, for example, it became clear how simple it is to exploit this technology for unethical purposes, such as spreading misinformation, impersonating political figures, and defaming innocent people [5].

However, it is also important to examine the possible positive aspects of this technology, to understand different facets of its development and eventually how to minorize the negative outcomes. An example of the educational use of artificial intelligence-generated videos is at the Shoah Foundation at the University of Southern California, which houses more than 55,000 video testimonies from Holocaust survivors. The university Testimony Project allows visitors to ask questions that lead to real-time responses from survivors in pre-recorded video interviews. In the future, this same technology will allow grandchildren to talk to artificial intelligence versions of deceased grandparents [6]. Deepfakes can also be present in the future of accessibility. Microsoft and Google are already developing AI synthetic voice to narrate real life and daily base objects. These narrations have the potential to help navigation apps for pedestrian travel, for example [7]. In the same vein that there are significant negative applications of deepfakes, the positive possibilities are also important to explore.

Sources

[1] Vaccari, C., & Chadwick, A. (2020). Deepfakes and Disinformation: Exploring the Impact of Synthetic Political Video on Deception, Uncertainty, and Trust in News. Social Media and Society, 6(1). https://doi.org/10.1177/2056305120903408

[2] Diakopoulos, N., & Johnson, D. (2021). Anticipating and addressing the ethical implications of deepfakes in the context of elections. New Media and Society, 23(7), 2072–2098. https://doi.org/10.1177/1461444820925811

[3] Fallis, D. (2021). The Epistemic Threat of Deepfakes. Philosophy and Technology, 34(4), 623–643. https://doi.org/10.1007/s13347-020-00419-2

[4] Mancuzo, R. (2022). Europol aponta que deepfakes serão muito usadas pelo crime organizado [Europol points out that deepfakes will be heavily used by organized crime]. Olhar Digital. https://olhardigital.com.br/2022/04/30/seguranca/europol-aponta-que-deepfakes-serao-muito-usadas-%e2%80%8b%e2%80%8bpelo-crime-organizado/

[5] Mirsky, Y., & Lee, W. (2021). The Creation and Detection of Deepfakes. ACM Computing Surveys. Association for Computing Machinery. https://doi.org/10.1145/3425780

[6] Debusmann, B. (2021). A evolução do deepfake, futuro da criação de conteúdo [The evolution of deepfake, future of content creation]. G1 Portal de Notícias. https://g1.globo.com/tecnologia/noticia/2022/04/07/a-evolucao-do-deepfake-futuro-da-criacao-de-conteudo.ghtml

[7] Jaiman, A. (2020). Positive Use Cases of Synthetic Media (aka Deepfakes). Towards Data Science. https://towardsdatascience.com/positive-use-cases-of-deepfakes-49f510056387

09

Exploring ESG & the Metaverse

Qiyan Emily WU

Department of Economics, UIC, Yonsei University

Although a lot of journals and articles have considered the practical uses and potential future of the metaverse, it was only recently when people began to consider it from the perspective of ESG. It appears however that the role of ESG can be a double edged sword in the context of the metaverse; it will be able to reduce material waste as virtual facilities and buildings are being built in the digital world, and reduce travel as virtual meetings reduce carbon emissions [1]. However, the dramatically increased amount of data processing and network traffic will affect electricity and power consumption.

From the environmental side, more and more firms have begun to adopt the method of digital twins; a virtual representation of objects in the metaverse that represent their existing products. For example, an energy-management firm based in Shanghai has introduced a new solution to infectious disease control by constructing relevant designs and infrastructure on the virtual collaborative environment [2]. From the perspective of governance and organizational structure, hierarchy and unbalanced work culture could be gradually reduced as everyone becomes equal in the digital world (though it is an open question whether this will be reflected in society). While ESG strategy is partially adopted to help the less advantaged and benefit overall society, the metaverse has not yet specifically addressed how it will incorporate nonprofits and charities. One of the criticisms of the metaverse is that it's very much profit-driven and emphasizes efficiency rather than non-profit generating matters that are nevertheless important in the real world.

Overall, one of the key questions is whether the creation of such a digital world can lead to a more sustainable one. Although the metaverse itself has been considered as a solution to reality and enabled continuous value-creation even without abundant tangible resources, the issue of sustainability still requires long-term effort. As the global vice chair of EY has noted, an important aspect is that "we need to address issues of accessibility, diversity, inclusion, and equity in the metaverse before they become ingrained [3]," firms and metaverse builders should look beyond the singular development of IT capability but towards a more diverse array of issues to enhance sustainability in both the real and digital world.

Sources

[1] Kwan, K. (2022, Jan. 10). ESG considerations in metaverse. Medium https://medium.com/@achworld-wideESG/esg-considerations-in-metaverse-e379993c4a8f

[2] BT News. (2020, Oct. 25). Dassault Sytemes, Aden Group launch hospital experience digital twin solution. Business Transformation. https://www.biznesstransform.com/dassault-systemes-aden-group-launch-hospital-experience-digital-twin-solution/

[3] Bianzino, N. (2022, Apr 7). Metaverse: could creating a virtual world build a more sustainable one? EY. https://www.ey.com/en_jo/digital/metaverse-could-creating-a-virtual-world-build-a-more-sustainable-one

10

Telemedicine to Telepsychology: The Evolution of Health Care

Yewon CHOI

Department of Economics, UIC, Yonsei University

Telemedicine is one of the major contributions of ICT. It has proven its worth especially as humanity tried to navigate through the COVID-19 crisis. Now telemedicine and remote treatment is branching out to encompass the mind. “Telepsychology”, “telemental health”, or online therapy, are new practices of caring for your mental health outside of the traditional office setting.

Telepsychology refers to the practice of “providing psychological services remotely, via telephone, email or videoconferencing [1].” Perhaps more so than for the body, online medical services for the mind are touted as an effective way to care for one’s mental health. This is because with the body, it is sometimes absolutely necessary for the doctor to see and assess with their own hands. However, in the case of emotional and mental distress, physical presence is less crucial. Online therapy is also especially helpful for those who live in rural areas that lack relevant facilities [1].

Like telemedicine, this new form of treatment has benefitted many individuals suffering from mental and emotional problems during the pandemic lockdowns. In strict terms, the virus can affect your body only if your body has it. For mental health, it can hurt you no matter if you have the disease or not. Factors of the pandemic that put one's mental health at risk include "separation from loved ones, loss of certain freedoms, uncertainty about the advancement of the disease and a feeling of helplessness [2]." Telemedicine offers a great amount of health for people in quarantine and people who feel insecure about visiting offline.

So far, the benefits of remote counseling are clear. But despite all the perks, there are some concerns. While accessibility is the greatest strength of telemedicine, it is also its greatest weakness. First, it was mentioned that telepsychology is a great alternative for those who live in areas without access to proper facilities. But for it to replace face-to-face meetings, you would most likely need an Internet connection and devices to connect you to your virtual therapy room. Rural areas, however, may be critically lacking in those kinds of infrastructure.

Another concern involves access to a safe and private space. Counseling, by nature, deals with sensitive information to keep confidential from families or friends. Therefore, those who seek therapy need to be in a place where they feel safe. If one were to visit a center in person, the walls of the therapy room serve as a protective barrier. However, if the person opted for an online session, they may not be able to pull out their deepest thoughts for fear of being overheard.

In any event, it is always a relief to have more options to choose from. The traditional method is nice if you have time and resources. But if not, never feel bad about choosing an alternative that technology is making possible.

Sources

[1] Novotney, A. (2011, June). A new emphasis on telehealth. American Psychological Association. https://www.apa.org/monitor/2011/06/telehealth

[2] Khalid, A. (2022, March 6). Mental well-being and tele-psychology. The News on Sunday. https://www.thenews.com.pk/tns/detail/938944-mental-well-being-and-tele-psychology

Barun ICT Global News

Publisher: Beomsoo KIM
Editors: Seungyeon WON, Alexandra STEPHENSON
Translators: Kyongju YU, Yeeun SHIN, Nahye HONG
Designer: Subin LEE

July 2022

** Please note that any external contributions to the Global News do not represent Barun ICT's official views.*

YONSEI UNIVERSITY

Barun ICT Research Center

Barun ICT Research Center, Yonsei University
50 Yonsei-ro, Seodaemun-gu, Seoul 03722, Korea
+82-2-2123-6694 | www.barunict.org

https://www.instagram.com/barunict/
https://www.facebook.com/barunict/