Barun ICT Global News

Global Student Reporter & Researcher

April 2021

Barun ICT Research Center

01 The Role of The State in Blockchain's Health Components

Jacklin Lee

Graduate School/Politics (Ph.D), Yonsei University

The advent of Blockchain technology was a breakthrough and gamechanger in the global market and various industries. The Bitcoin craze has drawn attention to cryptocurrency as part of the great fourth industrial revolution, but the Blockchain technology behind it has the bigger impact on political, economic, and social policies. For example, the technology is being considered for use in COVID-19 immunization programs. The biggest feature of Blockchain is "decentralization" and the reliance on anonymity has led to electronic transactions without government regulation. Whether it's a concern or a relief, people commonly believe that blockchain has shifted the influence of power from the government to individuals or private companies. However, all actors remain relevant, including the state.

Data can change – but with Blockchain, data is more immune from becoming outdated, large volumes can be more easily stored, privacy is more secure, and communication gaps and information sharing challenges can be overcome [1]. This is why health blockchain has advantages – and the state knows it too. In healthcare, states continue to play the key actor amidst the speculated decentralization.

Several countries have already started to utilize blockchain in the health sector. Surprisingly for the market speculators, it is the state who is leading this movement and governing the use and promotion of blockchain in health. The term "Digital 5" or "D5" has been named for the networking group of nations that are leading the digitized government with the goal of solidifying the digital economy since 2014, which include Estonia, Israel, New Zealand, South Korea, and the United Kingdom. The rough goals and agenda that the D5 states are advocating for include promotion of user needs, open standards, open source, open markets, open government, connectivity, coding education, assisted digital services, and commitment to share and learn [2].

Estonia was the first state to rely on a complete public health infrastructure operated on a healthcare blockchain. They have implemented migration of government data to blockchain technology aimed at securing access to more than a million health records to eradicate unauthorized access to these medical records bypassing the need of a centralized trust agent. In South Korea, major hospitals are also adopting this by collaborating with local public health clinics to launch a cloud-based information system supported by the government to help hospitals synchronize databases, adding to interoperability benefit [3]. In the United Kingdom, the National Health Service is utilizing blockchain for storing vaccines with sensors and cloud computing to remotely monitor the temperature of the refrigerators [4]. In all three countries, the states are not left behind, but are instead active actors when it comes to blockchain.

Bitcoin operates independently from the central bank through a peer-to-peer system. With blockchain, transactions can seemingly bypass the need for intermediary agents all over the globe. However, its role stretches to recordkeeping, tracking, monitoring, information-gathering, and storing data [5]. Bitcoin transactions may occur without the need for government intervention, but blockchain cannot occur without the promotion of the government. As the health sector is showing us more strikingly during the pandemic, blockchain technology does not oust the government, but continues to make it remain an important actor.

Sources

[1] Zhang, P. (2017). Design of Blockchain-Based Apps Using Familiar Software Patterns to Address Interoperability Challenges in Healthcare. 24th Pattern Languages of Programming.

[2] Ojo, A. & Adebayo, S. (2017). Blockchain as a Next Generation Government Information Infrastructure: A Review of Initiative Countries. Public Administration and Information Technology, vol. 32, pp 283-298.

[3] Alper, T. (2017, August 22). Government driving South Korea's blockchain progress. Crypto Insider. https://cryptoinsider.media/government-driving-south-korea-blockchain/

[4] Beard, S. (2021, March 1). Blockchain technology, used in Bitcoin, aids U.K vaccine program. Marketplace Morning Report. https://www.marketplace.org/2021/03/01/blockchain-tech-bitcoin-used-for-uk-vaccine-program/

[5] Swan, M. (2015). Blockchain: blueprint for a new economy. O'Reilly Media.

02 Smart Community Technologies Improve Digital Well-being in Light of COVID-19

Piao Wenling

Graduate School/Media Communication (Ph.D), Yonsei University

Smart community is one of the rising topics as companies and cities reframe their initiatives as "citizen-centric" in implementing smart city projects. Smart community technology can improve urban management, advance community goals, and enhance citizen's well-being in a smart city.

When COVID-19 hit, China deployed a wide range of smart community technologies such as face recognition, sensor networks, and communication technologies with artificial intelligence to support citizen's health, safety, and well-being. It is not only in preventing and mitigating the disease but also in prompting administrative orders to cope with additional outbreaks in the future.

iFlytek, a partially state-owned Chinese information technology company, launched its Smart Medical Assistant Telephone Robot to provide epidemic prevention information to residents of nearly 100 community health service centers in Tianjin, a municipality in northern China [1]. Through the service, citizens received voice calls, COVID-19 information, self-protection strategies, and other prompts. The robot can also assist with primary medical and health institutions to accurately evaluate lung lesions and their changes in patients with COVID-19[2]. Ele.me, an online-to-offline (O2O) catering and food delivery platform, launched fresh food self-delivery service stations within 11 neighborhoods in Wuhan. The company implemented self-pickup stations within 1 kilometer of the center area of the community. Residents only needed to click the "Buy food" button in the app, confirm the delivery time, and then be ready for pick up [3].

Smart communities deploy with the Internet, big data, artificial intelligence, and other new generation information technologies have greatly improved residents' digital living. With the extension of smart technology services from cities to communities, villages, and towns, smart communities have become a new focus in applying grassroots governance [1].

In recent years, China has been committed to smart cities in terms of smart community, smart governance, smart living, smart environment, smart mobility, and smart economy. In China's 13th five-year plan (2016-2020), 277 cities, including metropolises and rural areas, piloted smart city projects with $13 billion invested in deployment [4]. In China, the smart community is looming partially because of elderly care issues. In the proposals for the 2021 'two sessions'[1], two of China's techno giants Xiaomi and Baidu, made the case for promoting smart community technologies, including smart elderly care services, smart speakers, and smart technologies applied to elderly living scenarios to ease the woes of aging populations[5].

Despite its broad appeal, the privacy and security issues of citizens in smart communities remain incomplete. For example, the latest generation of deep-learning-based facial recognition fuels a loss of privacy [6]. In terms of the smart community, restricting entrepreneurs from data abuse and data-sharing with third parties requires more regulations and privacy policies.

N.B.

1. The "two sessions" also known as "lianghui" in Chinese are the most important political meetings of the year in which two main political bodies meet for planning.

Sources

[1] Gao, Q. (2021, Feb 2nd). Smart community building the digital living(智慧物业搭起生活服务圈).Cyberspace Administration of China website. http://www.cac.gov.cn/2021-02/02/c_1613837586979237.html.

[2] iFLYTEK. (2020, March 7th). IFLYTEK A.I. Image-Assisted Diagnostic Platform for COVID-19. iFLYTEK website. https://www.iflytek.com/en/news/88.html.

[3] Li, Z. (2020, March 23rd). Smart communities fight the pandemic(智慧社区，抗疫战中显“智慧”).Cyberspace Administration of China website. http://www.cac.gov.cn/2020-03/23/c_1586513834489563.html.

[4] IDG & Huawei. (2017). Huawei Smart City White Paper. Huawei Enterprise. https://e.huawei.com/en/material/industry/smartcity/9b0000e57fa94a2dbc0e43f5817ca767.

[5] China Daily (Edit.). (2021, March 6th). Two sessions: Ideas from tech entrepreneurs. Chinadaily.http://www.chinadaily.com.cn/a/202103/04/WS60401be1a31024ad0baac8fa.html.

[6] Hao, K. (2021, Feb 5). This Is How We Lost Control of Our Faces. MIT Technology Review. https://www.technologyreview.com/2021/02/05/1017388/ai-deep-learning-facial-recognition-data-history/.

03 Malaysia’s COVID-19 E-Tracer: A Double-Edged Sword

Muzaffar Bin Mahudin

Graduate School/Psychology (MA), Yonsei University

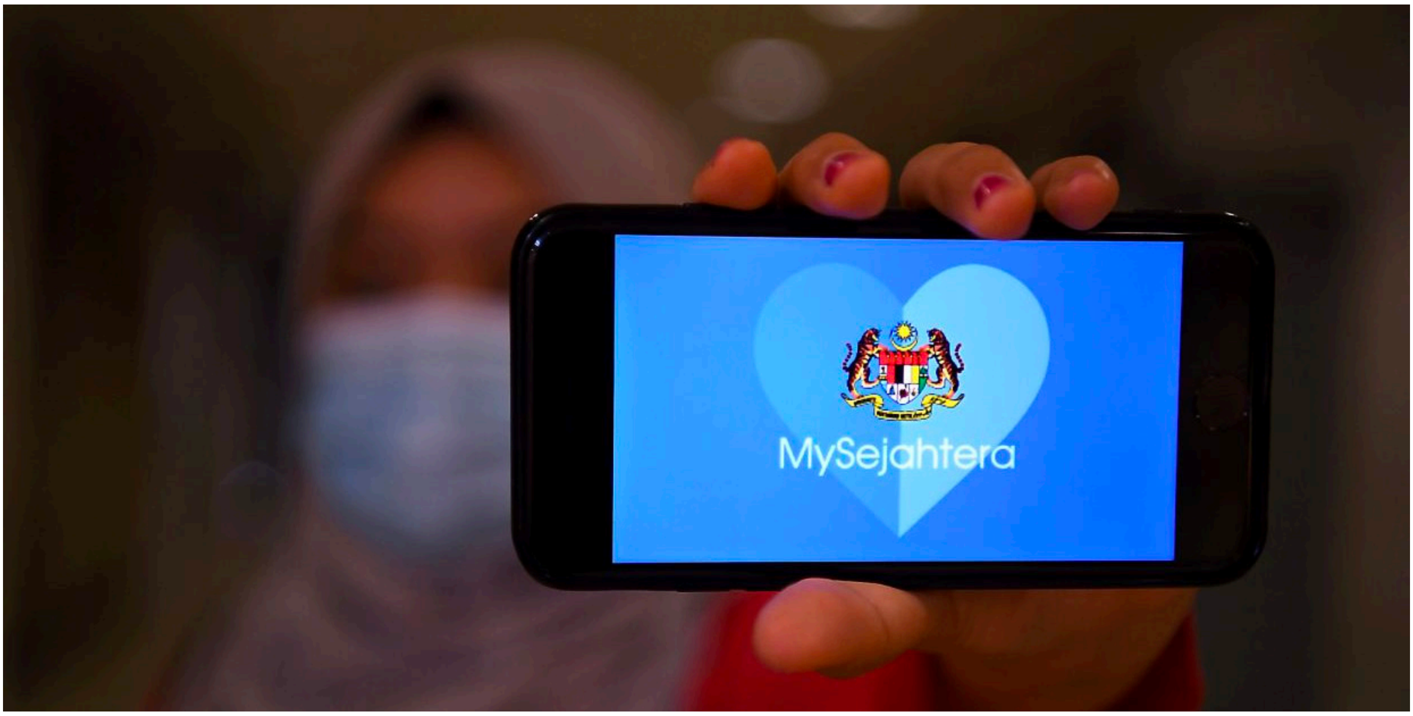

Image from https://www.thestar.com.my/tech/tech-news/2020/06/02/mysejahtera-apps-check-in-feature-now-live-stores-can-register-for-qr-codes

For every action, there is an equal and opposite reaction. Newton’s Third Law of Motion reflects the current situation in Malaysia on the use of the MySejahtera app, a mobile tracing application developed to curb the spread of COVID-19. To date, 42% out of 32.7 million people are using the app [1]. According to the Health Ministry, 311, 777 cases have been detected with a current trend averaging 1000 cases every day for two consecutive months [2]. The numbers remain high, hence the reaction from the government and the public on the effectiveness of the MySejahtera app are in question.

The Malaysian government reported that 9,127 cases have been detected through the app; 1,516 from the self-assessment features and 7,706 through database reviewing[3]. This report signified the benefit of the MySejahtera app to locate positive cases while convincing the public to keep using the app. Further, to ensure the safety and health of the public, the government implemented vaccination registration through the app to centralize the stages of the vaccination program. Malaysia has secured access to 110% of the vaccine enough to roll out the program to the entire population of Malaysia [4].

Despite government confidence, the public is concerned with the rate of successfully detected cases through the app. The app is mandatory for the public to enter any business and government premises yet the ratio between the number of active users and cases reported through it is insignificant after one year of implementation [1]. This proves only 6.1% of the users applied for the vaccination program [5].

What could lead to this major public distrust? The government has provided ample explanation with a variety of credible recommendations from experts on the functions of the app [1]. The answers may come from the legal issues on personal data protection [1] as well as public fear of the side-effects of the vaccine [6]. The government has promised all personal data will be stored for 90-days upon registration before being destroyed and it will not be shared with any parties for commercial purposes. However, if the data is leaked, the government does not hold accountability for the data breach and the public cannot take legal action against them [1]. The flame continues with public opinion on the need for vaccination as different vaccines have an inconsistent rate of effectiveness as well as the cases of side-effects of vaccines reported around the world [6]. The public distrust has stunted the app to serve as a medium between the government and the public to communicate on pressing matters.

The bridge must be connected. To flatten the curve means all parties must cooperate to ensure public health is the top priority. The government initiative to introduce the app during these uncertain times must be applauded. All public concerns are valid and must be addressed accordingly. To earn public trust, transparency is key.

Sources

[1] Kathirgugan, K. (2020, November 19) Has MySejahtera helped curbed Covid-19? Free Malaysia Today (FMT). Retrieved March 2021, from https://www.freemalaysiatoday.com/category/highlight/2020/11/19/has-mysejahtera-helped-curb-covid-19?/

[2] Ministry of Health. (2021, March 6). COVID-19 Malaysia updates by MOH. COVID-19 Malaysia. Retrieved March 2021, from http://covid-19.moh.gov.my/terkini

[3] DG of Health. (2020, November 21). Press Statement MOH Malaysia - Updates on the Coronavirus Disease 2019(COVID-19) Situation in Malaysia. Retrieved March 2021, from https://kpkesihatan.com/2020/11/19/kenyataan-akhbar-kpk-19-november-2020-situasi-semasa-jangkitan-penyakit-coronavirus-2019-covid-19-di-malaysia/

[4] Sipalan, J. (2021, February 16). Malaysia to kick off COVID-19 vaccination drive next week. U.S. Retrieved March 2021, from https://www.reuters.com/article/us-health-coronavirus-malaysia-vaccines-idUSKBN2AG05R

[5] Zolkepli, F. (2021, March 1). Only 6.1% of target 80% have registered for Covid-19 vaccine so far, says Khairy. The Star Online. Retrieved March 2021, from https://www.thestar.com.my/news/nation/2021/03/01/only-61-of-target-80-have-registered-for-covid-19-vaccine-so-far-says-khairy/

[6] Bernama. (2020, November 16). Govt monitoring anti-vaccine propaganda online. Free Malaysia Today (FMT). Retrieved March 2021, from https://www.freemalaysiatoday.com/category/nation/2020/12/16/govt-monitoring-anti-vaccine-propaganda-online/

04 Industrial Internet: Leading The New Era of Business Revolution

Jiyoung Song

Graduate School/Psychology (MA), Yonsei University

With the rise of the Industrial Internet, the world is on the threshold of a new era of innovation. The term "Industrial Internet of things (IIoT)" is a consolidation of the "Internet of Things" and "Big data" [1], indicating convergence of industrial systems enabled through advanced computing, analytics, cost-effective sensing, and a greater level of connectivity based on the Internet [2]. Unlike traditional supply chains following the simple process of production-supply-consumption, invention of IIoT has enabled digitalization of analog machines and service operations. Scientists have applied this high-tech information technology to numerous industrial machines, and it has minimized the use of unnecessary resources by predicting and avoiding possible stumbling blocks [3]. This simplified the acquisition of useful data and has connected not only machines but also people involved in business, therefore introducing a new business model to the industrial market.

The benefits from the use of the Industrial Internet will vary according to sectors, but there are common themes of risk reduction, fuel efficiency, higher labor productivity and reduced cost [1]. This is due to the fact that manufacturers can make the most rational decision to increase efficiency and productivity based on the great amount of data collected. Such innovations promise to bring greater speed and efficiency to industries as diverse as rail transportation, power generation, oil and gas development, health care service and even pizza delivery.

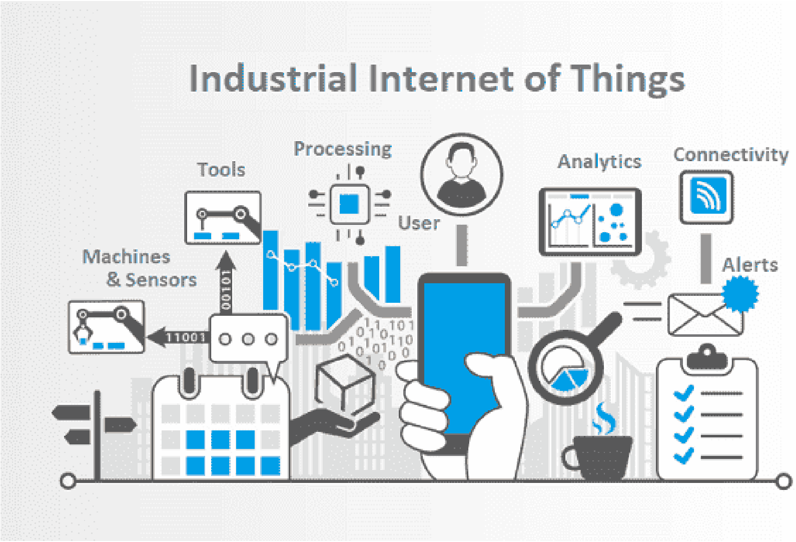

Image from https://www.rocknetworks.com/what-is-the-industrial-internet-of-things/

Like other commercial transportations, the airline industry is ideally positioned to further benefit from deployment of the Industrial Internet. By optimizing operations and assets while improving safety at every phase of the operation, application of IIoT has the potential to transform the entire airline industry. In particular, Southwest Airline utilizes IIoT to create service plans [4]. They would calculate the most suitable flight schedule, based on the data collected considering various variables such as temperature, humidity, wind direction, velocity, weight of air crafts, and the individual circumstances of each airport. This system has led Southwest Airlines to reduce aviation turbine fuel consumption, saving over one hundred million dollars.

Industrial business involves many actors including suppliers, distributors, producers, and developers and thus has been strengthening the network of these actors to build out its own ecosystem. One particularly salient example is the 'Smart + Connected City' project, currently expanding in the United States. AT&T, one of the leading telecommunication companies, has planned to launch a Smart City project through collaboration with high-tech corporations such as Intel, Cisco, and IBM [5]. The aim of this project is to monitor the real-time traffic situation of the city and assist the citizens with useful information such as arrival time of public transportation, notice for empty parking lots, and location of key facilities like police stations [5]. Recently, they have successfully transferred Atlanta's existing streetlights into a sensor-enabled data network [6]. By building a new system, IIoT aims to connect the entire world via digital networks, leading to a digitally ubiquitous society.

With the invention of Industrial Internet, the world is open to a new era of business revolution. However, since the technology is under the stage of development, they face a few limitations in commercialization. In this sense, the government should come up with new policies to standardize its application, facilitate convergence R&D, and establish legal systems to increase its competitiveness in the market.

Sources

[1] Munirathinam, S. (2020). Industry 4.0: Industrial internet of things (IIOT). Advances in computers, 117(1), 129-164.

[2] Boyes, H., Hallaq, B., Cunningham, J., & Watson, T. (2018). The industrial internet of things (IIoT): An analysis framework. Computers in industry, 101, 1-12.

[3] Iansiti, M & Lakhani, K. R. (2014). Digital ubiquity: How connections, sensors, and data are revolutionizing business. Harvard Business Review, 92(11), 19

[4] How big data and the Industrial Internet can help Southwest airline save $100 million on fuel (2016, July 9). Business Insider. Retrieved February 12, 2021 from https://www.businessinsider.com/sc/internet-helps-southwest-save-millions

[5] Burger, A. (2016, February 23) Three cities to showcase AT&T smart cities framework. Telecompetitor. Retrieved February 12, 2021 from https://www.telecompetitor.com/three-cities-to-showcase-att-smart-cities-framework/

[6] Power, G. GE, AT&T, Intel Pilot Sensor-Enabled data network with existing Atlanta streetlights (2019, September 26). Smart Cities Connect. Retrieved February 12, 2021 from https://smartcitiesconnect.org/georgia-power-ge-att-intel-pilot-sensor-enabled-data-network-with-existing-atlanta-streetlights/

05 The Dark Web: A Space for The Illegal Weapons Trade

Grecia Dominique Paniagua García

GSIS/International Cooperation (MA), Yonsei University

The internet is divided into two main platforms: the surface and the deep web. The surface web refers to all content that is accessible through a link, without security measures (such as all the information accessible on Google). While this is the most visible section, it only covers 2% of it. The deep web is all the information located behind security walls like passwords, credentials, or permissions. Typical examples of this section include emails, private, government, or corporate documents. The deep web constitutes 98% of the internet and here you can find the dark web. Constituting less than 1% of the internet, the dark web (also known as the dark net) is the smallest section in the deep web where most illegal activities take place. To access it, people need to use different browsers like Virtual Private Network (VPN) or Tor instead of Mozilla, Google Chrome, among others [1].

Terrorist organizations have taken advantage of the dark web to expand their activities including laundering money, publishing propaganda or manuals, and purchasing weapons (firearms, explosives, illegal materials). Even though it is not easy to link the weapons trade to the dark web, there are multiple occasions where intelligence has found that lone-wolf terrorist or big terrorist organizations buy their weapons online. One example is the mass shooting perpetrated at the Olympia Shopping Center in Munich in 2016. According to the German Federal Police, David Ali Sonboly bought a Glock 17 automatic pistol and 250 rounds of ammunition from the dark web [2].

How does this happen? What is the process behind weapons trade in the dark web? According to a report by the Office of Disarmament Affairs, terrorists purchase in two marketplaces: single-vendor markets and cryptomarkets. The first ones refer to online shops settled by individuals who trade specific products. Purchasing in these websites is not easy since finding reliable vendors on the dark web takes a lot of research and knowledge. Cryptomarkets refer to shop systems where there is a range of sellers for the same products. These sites include guidelines, discussion forums (such as in Amazon or Coupang) where buyers can research their purchases and give tips to other interested buyers. Compared to single-vendor markets, cryptomarkets are more reliable for buyers, and intelligence can monitor them more easily [3].

While this information sounds too confidential or alarming for the public, it is important to understand how the dark web markets operate. Most of the time, attacks (especially lone-wolf acts of terrorism) are unpredictable. However, scholars and intelligence organizations affirm that these attacks can be prevented if there is awareness of how perpetrators operate. At the same time, obtaining more information on how the dark web functions, could reduce the multiple challenges faced by law enforcement.

Sources

[1] Cybersecurity Spotlight – The Surface Web, Dark Web, and Deep Web. Center for Internet Security. Retrieved from https://www.cisecurity.org/spotlight/cybersecurity-spotlight-the-surface-web-dark-web-and-deep-web/

[2] Persi Paoli, G., Aldridge, J., Ryan, N., & Warnes, R. (2017). Behind the curtain. The illicit trade of firearms, explosives, and ammunition on the dark web. RAND. Retrieved from https://www.rand.org/content/dam/rand/pubs/research_reports/RR2000/RR2091/RAND_RR2091.pdf

[3] Persi Paoli, G. (2018, October). The Trade in Small Arms and Light Weapons on the Dark Web. UNODA. Retrieved from https://www.un.org/disarmament/wp-content/uploads/2018/10/occasional-paper-32.pdf

06 Proliferation of Apps Addressing Mental Health

Diego Buttigliero

GSIS/International Relations, Sogang University

COVID-19, with its concomitant social isolation, effects on the economy, and on people's bodies, has also had a notable influence on mental health. This has in turn affected the relationship between mental health and ICT. On the one hand, many responses were channeled through ICT - that is, the encounters between therapists and patients or various groups were 100% online. On the other hand, the crisis situation determined an increase in the demand for mental health, at the same time that it was moved towards the online world. This is reflected in the recent records of investments in mental health apps [1], and the growing proliferation of them. All this has notably increased the amount of raw data available on mental health, as well as the severity of conflicts related to privacy, the regulation of these types of apps, and the debates regarding their role in relation to mental health and subjectivity.

To focus on the topic of "mental health" apps, we can describe them according to their action programs [2]. Some of them track the symptoms of specific pathologies, such as depression or anxiety, administering tests with questions about mood, sleep, and recurring thoughts, and rating them. Others create diaries of emotional states, which are based on questions that evaluate emotions every day or week, and then make a graph of their evolution, which (they claim) can lead to the identification of symptoms and "situational triggers."

Then there are the apps for education on psychological issues, which provide general information ranging from specific conditions to general well-being, and which are operated from the input of questions made by the user. Then there are the chatbots that use artificial intelligence (AI) to accompany, ask questions and give recommendations based on the answers, usually from a platform that incorporates notions of cognitive behavioral therapy. There are also other apps that essentially function as conduits to therapists, acting as intermediaries. Others create online support groups of people with similar problems or symptoms.

Regarding these apps, it has been criticized that the vast majority of them are developed by commercial entities, while their relationship with professionals and mental health theories rarely appears explicit or centrally posted. This in turn has been related to the fact that the main channel of encounter of people with these apps are app stores and not health institutions [3]. These specific references, however, point to a much broader space for debate about whether there really is a positive effect on mental health, or some inherent relationship with it.

In a different position from these apps we can find developments linked to academic projects from psychiatry, such as an app that performs a certain type of discourse analysis to categorize a person's mental health status, that is based on machine techniques learning enabled by AI [4], creating new areas to for mental health professionals to consider and explore.

Sources

[1] Anónimo. (2020, December 15). Inversiones en apps de salud mental tocan récord alentadas por pandemia y uso de redes sociales. Retrieved February 23, 2021, from https://www.infobae.com/america/agencias/2020/12/15/inversiones-en-apps-de-salud-mental-tocan-record-alentadas-por-pandemia-y-uso-de-redes-sociales-2/

[2] Mental health app development: Making a scientifically credible app. (n.d.). Retrieved February 23, 2021, from https://madappgang.com/blog/mental-health-app-development-how-to-build-an-app-backed-by-science/

[3] Larsen, M., Huckvale, K., Nicholas, J., Torous, J., Birrell, L., Li, E., & Reda, B. (2019, March 22). Using science to sell apps: Evaluation of mental health app store quality claims. Retrieved February 23, 2021, from https://www.nature.com/articles/s41746-019-0093-1

[4] Want to know your mental health status? There's an app for that. (2020, February 06). Retrieved February 23, 2021, from https://www.colorado.edu/today/2019/11/12/want-know-your-mental-health-status-theres-app

07 COVID-19 Vaccine Cold Chain Faces Cybersecurity Risks

Hyunjoo Woo

UIC/Economics, Yonsei University

There is no doubt that the pandemic has accelerated connectivity in medical technology with the growing adoption of remote patient monitoring (RPM), AI-enabled decision support, and integrated command centers [1]. However, the pandemic has also heightened cybersecurity risks in the healthcare industry, and medical sectors are highly vulnerable to cyberattacks with far-reaching consequences. As vaccine rollouts continue around the world, hackers are taking advantage of the complex supply chain behind making and delivering vaccines.

Cybercriminals and Advanced Persistent Threat (APT) groups typically disguise themselves as credible entities and send phishing emails and malicious applications for various purposes such as commercial gain or initiatives to cause economic and civil disturbance. [2]. These cyber actors are taking advantage of the fact that in such an age of hyper-uncertainty, people are especially anxious about and focused on health-related matters. A frequent method they employ is sending SMS messages that lure users into clicking a link or downloading an application that leads to phishing websites. For example, a malicious Android app intended to track the outbreak was later discovered to trick users into downloading malware. A great number of victims also received emails including hyperlinks that lead to web pages that contain COVID-19-related wording within the URL (e.g., “corona-virus-business-update,” “covid19-advisory,” or “v19 support”) [3]. It is easy for victims to click on fake links and insert information that the mock pages require. This allows attackers to access the victim’s personal information such as financial account numbers and passwords, using them in malicious ways.

With such phishing methods, cyber attackers infiltrated the vaccine supply chain network through an outside provider with access to its systems. Cybercriminals impersonated an executive from Haier Biomedical, a legitimate member company of the COVID-19 vaccine supply chain and qualified supplier for the Gavi vaccine alliance's Cold Chain Equipment Optimisation Platform (CCEOP) program [4]. Disguised as an employee for the major cold chain provider, cyber attackers sent phishing emails to global organizations believed to be material support providers with the aim to "steal login credentials from those companies in order to gain future access to corporate networks and sensitive information relating to the COVID-19 vaccine distribution" the researchers said [5].

In response, IBM Security X-Force created a threat intelligence task force to detect all forms of cyber threats against organizations involved in the vaccine supply chain. Accordingly, IBM Security X-Force uncovered a global phishing campaign to ensure safe preservation of vaccines against any possible threats from cybercriminals [6]. The campaign aims to raise awareness of cybersecurity issues regarding the widespread distribution of vaccines and alert associated organizations of phishing attempts. After all, it is important to prevent disruption in the vaccine supply chains to optimize immunization equity and ensure appropriate response to emergencies. As vaccine roll out is a high priority in affected countries worldwide, companies managing the distribution should be attentive to potential cyber threats and strengthen their security posture moving forward.

Sources

[1] Bartlett, R., & Smit, N. (2020, August 18). Healthcare's connectivity cure? McKinsey & Company. Retrieved from: https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-blog/healthcares-connectivity-cure

[2] Threat Intelligence Team. (2020, April 9). APTs and COVID-19: How advanced persistent threats use the coronavirus as a lure. Malwarebytes. Retrieved from: https://blog.malwarebytes.com/threat-analysis/2020/04/apts-and-covid-19-how-advanced-persistent-threats-use-the-coronavirus-as-a-lure/

[3] COVID-19 Exploited by Malicious Cyber Actors. (2020). Cybersecurity & Infrastructure Security Agency.

[4] Gislam, S. (2020). Covid Vaccine Supply Chain Targeted By Hackers, Warns IBM. Industry Europe. Retrieved from: https://industryeurope.com/sectors/technology-innovation/covid-vaccine-supply-chain-targeted-by-hackers-warns-ibm/

[5] Lyngaas, S. (2020). COVID-19 hacking extends to supply chain for controlling vaccine temperature, IBM says. CyberScoop. Retrieved from: https://www.cyberscoop.com/coronavirus-vaccine-hacking-ibm/

[6] Zaboeva, C. (2020, December 03). IBM Uncovers Global Phishing Campaign Targeting the COVID-19 Vaccine Cold Chain. Security Intelligence. Retrieved from: https://securityintelligence.com/posts/ibm-uncovers-global-phishing-covid-19-vaccine-cold-chain/

Barun ICT Global News

April 2021

Publisher Beomsoo Kim
Editor-in-Chief Miyea Kim
Editor Seungyeon Won, Alexandra Stephenson
Translator Seungmin Baek, Yejin Juliet Yi, Kyong Ju Yu
Designer Siwan Kim, Ahyun Chung

* 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/