AN ASSESSMENT OF THE CHINESE COMMUNIST PARTY'S "MADE IN CHINA 2025" INITIATIVE ON TECHNOLOGICAL ADVANCEMENT AND ECONOMIC DEVELOPMENT IN THE AREA OF THE INTERNET OF THINGS

By: Hanh Nguyen, Celeste Clarke, Sahrash Tanveer, Zachary Risseeuw, and Brian K. Ngac, Costello College of Business, George Mason University

Introduction

The Chinese Communist Party (CCP) disclosed its “Made in China 2025” (MIC 2025) initiative as a state-led ten-year plan in 2015, which the goal is to advance high-technology production and implementation and to fortify and safeguard the nation's economy [1]. While the initiative focuses on ten significant sectors, in this paper, we focused on the Internet of Things as suggested by the U.S. Cyber Command’s representative who presented the research effort.

Internet of Things (IoT)

Oracle defines IoT as the network of physical devices that have sensors, software, and other technologies integrated into them so that they can communicate with other systems and devices over the internet and exchange data in real time [2]. In the 21st century, IoT products have become an essential part of our daily activities since they enable more convenience and better ways of collecting data from both consumers and enterprises perspectives. Spotting the benefits of IoTs, many countries have been investing more in IoT Research and Development (R&D) including China and the U.S. In this paper, we will focus on the IoT progress of these two countries.

Revenue and Investment in IoT by China and the U.S.

According to Statista 2022 report on IoT total market, China has reached nearly $120B in revenue, and is projected to be around $205B by 2025. In comparison, the U.S. IoT total market revenue in 2022 has reached $142.50B and is projected to be close to $225B in 2025. Additionally, the report on IoT investment shows that China has invested $1.21B, while the U.S. has invested $1.45B [3]. It can be seen that the gap between the revenues of China and the U.S. is considerably narrowing down from $23.5B to $20.7B. This signals a fast growth of China’s economy for the next a few years in IoT market, which can soon result in China possibly catching up with the U.S.

Top IoTs Companies

Besides well-known technology companies such as Huawei, Alibaba, and Tencent, China also has five “top” IoT-focused development companies including Quectel, Fibocom, Sunsea Group, China Mobile IoT, and MeiG Smart [4]. In comparison, the U.S.’ top five IoT development companies are Appinventiv, IBM, Accenture, Cisco, and Oracle [5]. These companies have a potential impact on shaping the two countries’ positions in the IoT industry within the next a few years.

Economy and High-technology Aspects

Now, almost every corner of China's cities has IoT products from transportation (e.g., bike sharing) to healthcare services [6]. From the perspective of the national economy, China seems to have a great amount of investment in developing smart cities devices to boost the IoT revenue and to define its existence in the world. In demonstration to China's presence globally, Huawei, the Chinese giant tech firm, has implemented a globalization strategy through establishing research labs and centers in London, Newbury, and Edinburgh within the United Kingdom in 2014, 2016, and 2017 [7]. The primary goal is not to enhance the export of smart city devices, but to build its presence in other countries beyond its own boarders. Similarly, China's expansion in Asian countries, especially in Southeast Asia, signals the significant reliance on China's IoT technology due to years of the established trading network [8]. This puts more pressure on the U.S. businesses when entering the Asian IoT market and impact the U.S. economy. Thus, China's economy has the possibility to surpass the U.S., or at least slow down the U.S. businesses in the IoT market since Asia has an enormous population - which accounts for 60% of the world's population.

Nevertheless, this dependency hints a cybersecurity problem that is created by those IoT devices and their obscured policies. Although, many Japanese and South Korean firms consider China as a vital partner, they still hold back their faith [8], which may affect China's plan on becoming dominant in this industry. Additionally, one reference shows that China is still challenged with its dispersed supply chain, various standards, and resistance to adopt industrial IoT devices [7]. Thus, in the most recent five-year plan, China devotes in forming its own supply chain to reduce its reliance on other countries' technology parts, especially the U.S.

As a late entry into the IoT market, the Chinese government tends to slow down other players through its policies and vast financial support. "China is likely to engage in protectionist and unfair trade practices to favor its own IoTs companies over foreign competitors, creating an austere and tacitly hostile market environment for foreign companies" [9]. Many foreign IoT businesses operate in China because of the low labor and land costs, and therefore,
the Chinese government seems to use regulations to restrict the growth of those businesses. In contrast, Chinese domestic IoT business will receive heavy support from the government to help the country improve its IoT industry. Besides national standards, China also attempts to influence international IoT standards despite its past failures.

Current Challenges

One possible concern followed by China's expansion in the IoT global market is authorized and unauthorized access of IoT devices or sensors that collect and possibly transfer users' data back to its manufacturing center. According to Smid, China collects data in four ways: 1 - by consent of its IoT product consumers, 2 - through the devices' design phase, 3 - by obtaining foreign companies along with their data, and 4 - through its government power that allows it to have control over the data collection [9]. Likewise, a vast entrance of Chinese IoT products may pose the threat of unauthorized access of weak configurations which results in secret data collection. Assuming that many U.S. citizens deploy China IoT products with inadequate configurations, China may easily observe and collect both consumers' and national data.

One past report shows that the "Chinese military and civilian researchers are energetically studying IoTs security vulnerabilities that could one day be built into trillions of IoTs devices manufactured to comply with China's preferred international standards" [10]. In the most recent event's response to this concern, "Senators Mark Warner and Rick Scott have put forward the American Security Drone Act of 2023" [11]. This was due to the potential national security implications if the images and videos captured by many U.S. police departments who use DJI drones (a private Chinese technology company) were sent back to Beijing.

IoT Applications

From the IoT application in high-technology perspective, China has visioned the application into space activities including "an integrated network of communications, Earth observation and navigation satellites" [9]. With this, China may deploy IoT military-based applications which could negatively impact other countries' military activities [9]. For Example, an unmanned aerial vehicle (UAV), can be used by the military to navigate remotely capture activities such as troops' practices from the sky. These UAVs are embedded with IoT sensors and software that help connect to the network and transmit data[12]. Thus, these raises concerns of vulnerabilities such as Man-in-the-middle (MITD), which would result in unauthorized access to confidential systems and data.

Together with the growth of 5G which provides faster and smoother connectivity for smart devices produced by China, it is likely that China becomes the dominant entity in the IoT space. China has a large and almost-complete 5G national network and with its large population, China will be able to collect more user data and find potential vulnerabilities faster than before. As mentioned above, the three giant technology companies are holding a critical role in boosting national IoT applications, as well as building influences on international standards. To illustrate, Huawei is reported as an essential provider for 5G technology in most of the Chinese smart city projects. This company also develops its own supply chain of hardware and software when it got into the U.S.' sanction under the former president Trump's administration, a case of Harmony operation system that is used in IoT application [13].

Additionally, AI development works side by side to enhance and manage the IoT applications in China, especially in the smart cities context. Alibaba has been successful in bringing the AI and IoTs applications together in a smart city project called "City Brain," which involves traffic, transportation, and environment management systems [13]. This project is successful in Hangzhou city and will even be adopted in Malaysia. Nevertheless, this will possibly draw businesses away from the U.S. technology companies that can affect our national economic expansion and enhance China's presence in international IoT standard setting and market.

Potential Solutions for the U.S.

The U.S. federal and state governments should quickly work toward solutions that help to mitigate the impact of the challenges mentioned, especially when China's presence and influence have become more visible. There are four ways that the U.S. government may consider implementing as follow [9]. First, they can put more pressure on data privacy and security law to restrict Chinese IoT companies and products on entering a national market. For instance, the U.S. recently did so with TikTok that is owned by Byte Dance, a Chinese company. [14] Second, the U.S. should encourage states to engage more in international standard bodies to ensure that these standards will not be shifted toward any other country's advantage. Third, there should be more programs that attract and welcome more experts, scientists, and talents to enhance national IoT innovation and development. Fourth, the U.S. government should consolidate relationships with our allies to prevent China's penetration and exchange research, practices, and experiences for better IoT improvement.

Conclusion

Although we do not know the result of "Made in China 2025" Initiative yet since it is still in progress, we can predict that China is moving very well toward their target in the next a few years. To safeguard our nation's leading position in the world, we should maintain our active presence in diplomacy and the world economy. Thus, we should pay more attention to the IoT sector where we set standards and requirements; at the same time, invest in the country's next generation of cyber warriors through education, training, and research and development.

References

[1] McBride, J., & Chatzky, A. (2019, May 13). Is “made in China 2025” a threat to global trade? Council on Foreign Relations. https://www.cfr.org/backgrounder/made-china-2025-threat-global-trade

[2] Oracle. (n.d.). What is the internet of things (IOT)? What Is the Internet of Things (IoT)? https://www.oracle.com/internet-of-things/what-is-iot/

[3] Internet of Things - China: Statista market forecast. Statista. (n.d.). https://www.statista.com/outlook/tmo/internet-of-things/china. Mason Access

[4] Yang, Y. (2023, July 26). Review: 12 leading Chinese companies in the IOTS module industry. EqualOcean. https://equalocean.com/analysis/2023072619974

[5] TBN Team. (2023, August 22). Top 10 US IOT Software Development companies 2023. Tech Business News. https://www.techbusinessnews.com.au/blog/top-10-iot-software-development-companies-in-the-usa-2023/

[6] Komarraju, A. (2021, February 22). China might become the world’s IOTS industry leader in 2024. Analytics Insight. https://www.analyticsinsight.net/china-might-become-the-worlds-IoTs-industry-leader-in-2024/

[7] Atha, K., Callahan, J., Chen, J., Walz, E., Drun, J., Green, K., Lafferty, Dr. B., McReynolds, J., Mulvenon, Dr. J., & Rosen, B. (2020, January). China’s Smart Cities Development. https://www.uscc.gov/sites/default/files/2020-04/China_Smart_Cities_Development.pdf

[8] Lee, J. (2021, December 8). The internet of things: China’s rise and Australia’s choices. Home. https://www.lowyinstitute.org/publications/internet-things-chinas-rise-and-australias-choices

[9] Smid, H. H. F. (2023, April 17). Internet of things: The China perspective. The Space Review. https://www.thespacereview.com/article/4566/1

[10] Chen, J., Walz, E., Lafferty, B., McReynolds, J., Green, K., Ray, J., & Mulvenon, J. (2018, October). China’s internet of things - inside cybersecurity. https://www.uscc.gov/sites/default/files/SOSi_China’s Internet of Things_Executive Summary.pdf

[11] Brewster, T. (2023, June 2). Exclusive: U.S. states are flying thousands of Chinese drones across the East Coast. Marco Rubio is furious. Forbes. https://www.forbes.com/sites/thomasbrewster/2023/06/01/american-states-fly-thousands-of-chinese-drones-across-east-coast/?sh=2017440e6495

[12] Guilmartin, J. F. (n.d.). Unmanned Aerial Vehicle-Military Aircraft. Encyclopedia Britannica. https://www.britannica.com/technology/military-aircraft/Fighters Last updated April 23, 2024

[13] Fowle, H. (2023, December 7). IOTS’s china conundrum. IOTS Insider. https://www.IoTsinsider.com/news/analysing-chinas-ascendancy-in-the-IoTs-landscape/

[14] Fung, B. (2023, March 21). Lawmakers say tiktok is a national security threat, but evidence remains unclear | CNN business. CNN. https://www.cnn.com/2023/03/21/tech/tiktok-national-security-concerns/index.html

About the Authors

Hanh Nguyen is pursuing an undergraduate degree at George Mason University in Business with concentration in Management Information System and is a member of Honors Program. She is interested in programming.

Celeste Clarke is a senior student and a member of Honors Program at George Mason University and pursuing a bachelor’s degree in management information system. She has been an independent investor for 19 years. Celeste is interested in French, network security, and cloud computing.

Sahrash Tanveer is an undergraduate student at George Mason University, pursuing a degree in Business Administration with a concentration in Management Information Systems. She is a member of the Honors Program and is interested in data analytics and cloud computing.

Zachary S. Risseeuw is a Business Technology Solutions Analyst at Deloitte Consulting within its Government & Public Services practice. Zach received his Bachelor of Science summa cum laude from George Mason University with a major in Business Analytics and a minor in Legal Studies. Prior to graduating, he interned at the U.S. Department of the Navy’s Office of the Assistant Secretary.

Brian K. Ngac, PhD is an Instructional Faculty Member and Dean’s Teaching Fellow at George Mason University’s Costello College of Business. He’s the Founding Director of the Professional Readiness Experiential Program (PREP) where Honors and High-Performing Students work on real projects with real industry participants to gain hands-on experience prior to their graduation. Any interested organizations that would like to be an industry participant are encouraged to contact Brian at bngac@gmu.edu