An Analysis of the "Made in China 2025" Initiative with U.S. Cyber Command

A Professional Readiness Experiential Program (PREP) Project Effort

----- ***Authors / Student Project Team Members*** -----

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 (Fairfax, Virginia, USA) with a major in Business Analytics and minor in Legal Studies. Prior to graduating, he interned at the U.S. Department of the Navy's Office of the Assistant Secretary (Financial Management and Comptroller).

Celeste Clarke is a senior student and a member of Honors Program at George Mason University (Fairfax, Virginia) and pursuing a career in Management Information System. She has been an independent investor for 19 years. Celeste is interested in French, network security, and cloud computing.

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.

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.

----- ***Industry Participant / Mentor*** -----

Sean Hoey
United States Cyber Command

----- ***Faculty Member*** -----

Brian K. Ngac, PhD
Instructional Faculty & Dean's Teaching Fellow
George Mason University's Costello College of Business
bngac@gmu.edu

Interested in being an Industry Participant and or PREP Sponsor? Please reach out to bngac@gmu.edu, Thanks!

---- Client Testimonial ----

"This semester's PREP team did an excellent job extensively researching and providing unique insights into the status of several complex high-technology sectors within China. This work helped provide a survey of available information and foundational analysis into priority topics of interest that will almost certainly prove useful throughout the organization. The PREP students were responsive, engaging, and a pleasure to work with."

- Sean Hoey | United States Cyber Command

Introduction

The U.S. Department of Defense's (DOD's) 2022 National Defense Strategy identifies the People's Republic of China (PRC or China), in the words of Secretary Lloyd Austin, as the country's "most consequential strategic competitor for the coming decades" [1]. In 2015, the Chinese Communist Party (CCP) unveiled its "Made in China 2025" (MIC 2025) initiative, a state-led 10-year plan that aims to develop the country's industrial base by advancing high-technology production and implementation while strengthening and protecting its economy [2]. MIC 2025 focuses on 10 key high-tech sectors ranging from bioengineering to maritime engineering and includes the four sectors that we will analyze herein: quantum computing, artificial intelligence/machine learning (AI/ML), Internet of Things (IoT), and aerospace equipment [2]. We have conducted our research and completed our writing in collaboration with U.S. Cyber Command; thus, we will analyze the sectors at hand from a cyberspace perspective. The Office of the Director of National Intelligence (ODNI), in its 2024 Annual Threat Assessment, asserts that "China remains the most active and persistent cyber threat to U.S. Government, private-sector, and critical infrastructure networks" [3]. With this in mind, we seek to evaluate the pertinent topic of China's cyber advancement via MIC 2025 on the global geopolitical landscape.

1. U.S. Department of Defense, "2022 National Defense Strategy," 27 October 2022, https://media.defense.gov/2022/Oct/27/2003103845/-1/-1/1/2022-NATIONAL-DEFENSE-STRATEGY-NPR-MDR.PDF
2. McBride, J.; A. Chatzky; "Is 'Made in China 2025' a Threat to Global Trade?," Council on Foreign Relations, 13 May 2019, https://www.cfr.org/backgrounder/made-china-2025-threat-global-trade
3. U.S. Office of the Director of National Intelligence, "Annual Threat Assessment of the U.S. Intelligence Community," 5 February 2024, https://www.dni.gov/files/ODNI/documents/assessments/ATA-2024-Unclassified-Report.pdf

Business Challenge

US Cyber Command tasked the team with analyzing 4 sectors: Quantum Computer, Artificial Intelligence / Machine Learning, the Internet of Things, and Aerospace Equipment. Specifically, a compare and contrast analysis between China and the United States focused in the areas of Investments and Achievements, Current Challenges, Potential Applications, and Economic and Technology Prediction.

Activities Done to Address the Business Challenge

The Team's research and in-depth analysis are formulated into an unpublished collection below in the next 21 pages.

Results & The Positive Impact

Out of the analysis, the team was able to get two of their focus areas published by the Information Systems Security Association Journal (Quantum Computing and the Internet of Things).

An Assessment of the Chinese Communist Party's "Made in China 2025" Initiative on Technological Advancement and Economic Development

The U.S. Department of Defense's (DOD's) 2022 National Defense Strategy identifies the People's Republic of China (PRC or China), in the words of Secretary Lloyd Austin, as the country's "most consequential strategic competitor for the coming decades" [1]. In 2015, the Chinese Communist Party (CCP) unveiled its "Made in China 2025" (MIC 2025) initiative, a state-led 10-year plan that aims to develop the country's industrial base by advancing high-technology production and implementation while strengthening and protecting its economy [2]. MIC 2025 focuses on 10 key high-tech sectors ranging from bioengineering to maritime engineering and includes the four sectors that we will analyze herein: quantum computing, artificial intelligence/machine learning (AI/ML), Internet of Things (IoT), and aerospace equipment [2]. We have conducted our research and completed our writing in collaboration with U.S. Cyber Command; thus, we will analyze the sectors at hand from a cyberspace perspective. The Office of the Director of National Intelligence (ODNI), in its 2024 Annual Threat Assessment, asserts that "China remains the most active and persistent cyber threat to U.S. Government, private-sector, and critical infrastructure networks" [3]. With this in mind, we seek to evaluate the pertinent topic of China's cyber advancement via MIC 2025 on the global geopolitical landscape.

Quantum Computing

Quantum computing is known as supercomputing or also understood "as specialized computers that can solve specialized problems set at an extremely fast rate such as complex optimization problems or molecular modeling, that current computers cannot." [4] It uses qubit instead of bit which is used in traditional computing. Even though quantum computing is not fully developed yet, many nations have entered the race to develop their own quantum computing which can serve in many sectors from medicine, business, science, computing, and communication to national defense system. According to Penney, "Quantum computers may also be more efficient and faster at highly complex artificial intelligence/machine learning algorithms, but there are also many use cases where classical (or traditional) binary computing delivers faster and more accurate solutions." [4]

Investment and Achievements

China has invested billions of dollars in Quantum computing in recent years. They have attracted many physicists and scientists around the world to help them build complete made-in-China quantum computers by heavily funding quantum computing sector. For example, the United States committed to fund an additional $1.8 billion in quantum computing while China also announced that it would invest "$15.3 billion" [5]; however, according to Freedberg, maybe China only invested about "$4 billion or even less" [6]. China's actual investment in quantum computing remains unclear until today.

Quantum computing is a new technology race for many nations. Thus, many startups to giant tech firm have entered this field. There are thirty active quantum computing companies in China. China currently has nine major companies such as Baidu Research, Ciqtek, Huawei Cloud,

Origin Quantum, Qasky, Quantumctek, Qudoor, Tencent Quantum Lab, ZTE. Those companies focus on applying quantum computing in search engines, cloud computing, online business platforms, software solutions, network security, and quantum cryptography communications [7].

The U.S. surpass China in both the number of quantum computing companies and patents. Currently the U.S. has over "110 public and private quantum computing companies with over 1086 patents" versus "30 companies and 384 patents in China" [8]. Giant technology firms such as Google, Microsoft, Intel, and IBM have invested dramatically in this field. According to Pichai, the CEO of Google, it was "the first company" to launch a strong complete quantum computer in 2019 after 13 years of research and development [9]. For example, "Google recently achieved quantum supremacy by solving a problem in 200 seconds that would take a classical computer 10,000 years to solve." [10] In response to this event, China claimed that they have successfully built two complete quantum computers which is much stronger than the one Google built; however, China did not provide any evidence to support their claim.

Potential Application

Quantum computing has vast promising future applications varying from medical field, business services to national defense system. According to Amerongen, a co-author of NATO's White Paper on Quantum Technologies, the focus of quantum computing will be on quantum sensing, quantum communication, quantum computing, implications for defense and security. [11] First, quantum sensing can increase the precision of medical imaging and diagnosis which helps detect ailments in the early stage, so medical physicians deliver more accurate treatment schedules and medication to shorten the treatment time and save more lives. For instance, "… quantum sensors can detect subtle brain activity changes, aiding in the diagnosis and monitoring of neurological disorders [20]. Similarly, in cardiology and oncology, quantum-enhanced imaging techniques provide valuable insights into heart conditions and cancer detection." [12]

Second, quantum communication used qubit which is more secure than bit in optical fiber cables in traditional internet. According to Amerongen, when hackers try to steal data by interrupting data during its transmission, quantum communication channel will collapse which means hackers cannot steal data since "quantum computing is extremely sensitive to external disturbances." [11] Quantum communication opens the door for ultra-secure data transmission via the internet since data becomes un-hackable in quantum communication which creates a much safer channel for transferring data in the future.

Third, quantum computing can simulate drug discovery and new materials, solve complicated optimal solutions in logistics and finance. Additionally, it combines artificial intelligence for advanced machine learning and applies to asymmetric encryption algorithm for secure data transmission. "Big technology companies like IBM, Google and Microsoft are racing for 'quantum supremacy.'" [11] It is a point where a quantum computer succeeds in solving a problem that no classical computer could solve in a super short given time.

Fourth, implications of quantum computing for defense and security are extremely important in any defense system. According to Smith-Goodson, "Once fully developed, quantum radar could threaten the US lead in stealth technology. That translates into the increased vulnerability of US stealth aircraft such as the B-2 Spirit, F-22 Raptor, F-35 Lightning II, and allied stealth aircraft. Quantum radar might also be able to determine the type of aircraft or the weapons the plane is carrying. It could also compromise US domination over the electromagnetic domain in combat environments." [10]

However, during the 118th Congress Hearing on Current and Emerging Technologies in U.S.-China Economic and National Security Competition, Thursday, February 1, 2024, Freedberg Jr. stated that the U.S. ruled out quantum radar and quantum key distribution (QKD) technologies while China has invested heavily on them. Experts predicts that this could be bad bets for China since "the U.S. military has publicly identified quantum radar as impractical." [6] He wrote "My own assessment largely agrees with the U.S. DoD's position that QKD and quantum radar are unlikely to deliver significant military operational advantage." [6]

In short, quantum computing technologies help increase the security and ability of detecting objects in air, land, and water. These technologies will have a huge impact on future economy and defense systems for any nation.

Current Challenges

One of the challenges of quantum computing is the amount of heat that quantum computers release during their operation. Chinese companies have successfully developed a device called EZ-Q Fridge. "The EZ-Q Fridge is designed to provide an ultra-low temperature environment, nearing absolute zero Celsius, crucial for the optimal performance of quantum computing chips." [13] Chinese companies enjoyed the success of their research and development as it performed well in testing and those companies have begun deliveries of this refrigerators to their customers starting in the second quarter of 2023. However, no one has heard about how effective EZ-Q Fridges are in actual applications ever since.

The U.S. researchers are in testing phase for a new cooling technology for quantum computing. According to Toon, "A new cooling technique that utilizes a single species of trapped ion for both computing and cooling could simplify the use of quantum charge-coupled devices (QCCDs), potentially moving quantum computing closer to practical applications." [14] This promising technology can be used to produce a cooling system for any device or system that uses quantum chips.

Economic and Technological Prediction

Although quantum computing is still in its infancy stage, investors around the world have already started investing in quantum computing companies varying from start-ups to giant tech firms. According to Williams, the investment in this market was nearly $500 million in 2021 but it is expected to reach nearly $1.7 billion by the end of 2026. [15] Quantum computing seems to set the run for the fifth industrial revolution. In addition, Bogobowicz et al., predicted that "… the four industries likely to see the earliest economic impact from quantum computing—

automotive, chemicals, financial services, and life sciences—stand to potentially gain up to $1.3 trillion in value by 2035." [5]

Quantum computing application in medical field may lead to advance technologies in treatment and medicine which would draw people to the U.S. for medical tourism. According to Precedence Research, the global medical tourism market is predicted to grow very fast from $116 billion in 2022 to more than $346 billion in 2032 [16] It triples its market value within a 10-year period. Medical tourism has become very popular in the last decade since wealthy people still want to get advanced medical care such as high technology, advanced medicine, and better services. It is one of the most attractive markets that contributes a good income to a nation's economy which helps boost other sectors of the economy such as retail, other services, hospitality, and tourism industry.

"In 2022, GlobalData said the U.S. was about five years ahead of China in the quantum computing race. Now, in 2024, the firm considers the two countries as "nearly equal" in the arena." [17] The quantum computing race is now nearly tied between the U.S. and China; however, the U.S. is behind with around 45 thousand versus China with nearly 58 thousand [5] when it comes to the number of quantum computing talents. Still the question is how the quality of quantum talents is still open since people do not know how much the gap between Chinese quantum talents and U.S. quantum talents is.

The post-quantum cryptography (PQC) algorithms standard may be released in 2024. The National Institute of Standards and Technology (NIST) is in its final process to finalize a new standard for PQC communication encryption which cyberspace experts believe would provide long-term security for cyberspace communication. According to NIST, "The agency has begun the process of standardizing these algorithms — the final step before making these mathematical tools available so that organizations around the world can integrate them into their encryption infrastructure." [18]

Quantum computing threatens our nation's safety. The ability of combining two quantum computers to increase their power imposes a threat to our national defense system. According to Sanzeri, China has proven the "ability of entanglement sub-atomic particles and maintain them over twelve kilometers" [19] which also means that quantum power can be used as a threat to crack standard encryption that our current defense system uses.

Recommendations

As mentioned above, China surpasses the U.S. in the number of quantum computing talents which means they have more scientists and physicists than the U.S. Therefore, U.S. should attract more quantum talents starting with nurturing the next generation of the country, funding high schools, colleges, and universities by providing excellent mathematics and science education programs to attract more students in this field. In addition, we should facilitate visa program for quantum talents around the world who are currently studying in the U.S. or planning to come to the U.S. for studying and research in this field. Working permits should be granted to quantum talents so they can stay in the U.S. for work after their graduation.

According to Kitchen and Drexel, the U.S. should establish "stricter patent protections and more aggressive repercussions for domestic and international offenses in IP theft" [20]. The U.S. Defense Department should maintain partnerships with private sectors as they have been doing in the last decade along with collaboration with our allies around the world in quantum computing research and development.

The U.S. should monitor the supply chain of exporting critical components and materials of quantum computers and also create an ecosystem where the government pays attention to the financial health of small, specialized quantum computing firms.
According to Dargan, "Baidu's vision encompasses the widespread integration of quantum technology across diverse sectors, including artificial intelligence (AI) and machine learning (ML)." [21]

Artificial Intelligence / Machine Learning (AI/ML)

China, along with the rest of the world, experienced unprecedented economic challenges in the wake of the Covid-19 pandemic. This makes economic analysis of a plan slated for implementation between the years of 2015 and 2025 unique. On a macro level, China's "modest" 2023 economic growth (5.2% increase in GDP) combined with recent indicators of deflation signal slowing economic development that contrasts to the strong growth of prior years and decades [4]. At a minimum, an assessment points to uncertainty over the trajectory of China's economy, and some methods of evaluation point to a downward trajectory [4].

In assessing MIC 2025's impact on Chinese economic development overall, it is important to note that although the initiative, reliant on financial stimulus, was prominently unveiled, the CCP "never publicly identified" the companies it intended to infuse with funds [5]. After some time, "diplomatic backlash" over MIC 2025 caused China to keep the name of the initiative out of its vocabulary, but the underlying objectives have stayed the course [6]. Consequently, in conducting an analysis of the actual effects of the policies involved, researchers at the Centre for Economic Policy Research scoured open-source financial data from companies with publicly mentioned ties to MIC 2025 and found "little statistical evidence of productivity improvement or increases in ... profitability measures," reaching a conclusion that it is unlikely MIC 2025 "has achieved its key objectives" [5]. Coupled with "strong evidence" that the Chinese economy has incurred substantial costs due to MIC 2025, it is relatively clear that the initiative has not lived up to its ambitions on this front [5].

The Prominence of AI

Gregory Allen, Director of the Center for Strategic & International Studies' (CSIS') AI Center, in September 2023 testimony before the U.S. Senate, stated, "The senior military leadership of both the United States and China believe that AI will be foundational to the future of military and economic power" [7]. He explained that AI and the machine learning it runs on is a "general-purpose technology" [7]. Like other technologies over the years, he continued, while the implementation of AI for military purposes is already serving some useful applications, it will come to fundamentally transform military operations over future decades [7].

A Take on History and Governance

Stepping back, while authoritarianism typically lags democracy in cutting-edge technological development, the proliferation of AI in China might not be subject to that general pattern [8]. Harvard Professor David Yang points to the reason for "the outsized success of China's AI sector" as an inherent overlap existing between the abilities of this type of technology and the interests of an authoritarian government [8]. Such governments, keen on monitoring their citizens, would probably like to even predict aspects of their citizenries, and AI provides that potential [8]. The vast collection of data by such governments puts them in places to rapidly develop AI, a technology heavily dependent on data, and so a natural fit exists [8]. Harvard Professor Yuhua Wang argues, nevertheless, that by looking at the history of Ancient Chinese governments, instability within the elites at their top levels caused regime volatility, and that could lead to "a very dramatic but also gradual decline of the capacity of the Chinese state" [8]. These more qualitative notions are useful to keep in mind through this more quantitative analysis.

The Chinese AI Market

Looking at the AI market specifically, outlooks forecast China's generative AI application market to increase by a compound annual growth rate (CAGR) of 46% from 2022 to 2025, and its AI digital commercialization market to increase by a rate of 55% over that period [9]. The main driver of those growth figures is said to be AI digital services, which themselves are expected to grow by a CAGR of 55% over those years [9]. Citigroup caveats these apparently impressive statistics, however, by clarifying that uncertainty remains regarding how "these forecasts would translate into monetization opportunities or incremental revenues" for Chinese chatbot companies [9]. The International Data Corporation (IDC) estimates that China's AI software and application market will grow by a CAGR of 32.9% from 2021 to 2026, and Citi Research predicts that this will "revolutionize" the country's SaaS industry [9]. Focusing on cybersecurity, IDC estimates that China's cybersecurity market will grow "at a fast CAGR of 21.2%" from 2021 to 2026 [9]. To put this into context, the global cybersecurity market is more developed and is estimated to achieve "a stable 11.3% CAGR" from 2021 to 2026 [9].

Taken together, although these figures appear impressive in the abstract, paying particular attention the relatively high cybersecurity growth rate compared to the rest of the world indicates that China is behind in an earlier growth stage considering the world's achievement of maturity.

A Major Piece of the Puzzle: Chips

In addition to the software involved with the functioning of AI, hardware represents the other part of the equation, and as Allen of CSIS states, the U.S. and its allies have a "significant technological edge" in this area [7]. Semiconductor chips are the main hardware elements to consider, and Allen asserts that the most effective way by which China can progress in its AI capabilities is to use American chips, as it has in the past [7]. George Mason University Professor Robert Deitz, former General Counsel of the National Security Agency (NSA; concurrently led by the commander of CYBERCOM), put it quite simply (and rhymingly): "Why make it yourself when you can steal it from someone else?"

To set the stage, a major turning point occurred in 2022 when the Biden administration implemented a new export policy aimed at hampering China's ability to access U.S. semiconductor technology [7]. However, the U.S.' main enforcement mechanism of export controls lies in the Department of Commerce's Bureau of Industry and Security (BIS), which Allen says has faced chronic underinvestment and is not properly positioned to execute its mission [7]. To be most successful, the U.S. should implement stricter export control policies in tandem with the likes of the Netherlands and Japan to avoid slip through of technology to China [7]. It is only in this holistic manner that meaningful results can be achieved.

All the Buzz: Generative AI

As of February 2024, numerous tech and engineering insiders and experts placed China "at least a year" behind the U.S. in its generative AI capabilities, a reality acknowledged within China itself [10]. Chinese tech companies racing to build generative AI platforms "are relying almost entirely on underlying systems" from U.S. entities, and these subject matter sources indicate that the gap between China and U.S. may be widening [10].

So, in assessing the totality of the circumstances, some indicators point to China being ahead of the US, particularly regarding the broader tech battle, but most analysts and experts suggest that the U.S. is considerably ahead of China in the AI arena.

Keeping an Eye Out: AI Regulation Development

China is developing "some of the world's earliest and most detailed regulations governing" AI [11]. There is a tendency in the West to dismiss or view as strictly competitive China's regulatory advancements in this area [11]. However, there is a strong argument made that even if there is disagreement in approach, much can be learned between countries [11]. China is working its way from piecemeal regulation-making to the establishment of a "capstone national AI law," much like the process which built up to the establishment of its pivotal 2017 cybersecurity law [11]. This ties into the U.S. needing to watch closely while progressing its own regulations considering the concept of technological "ecosystems" that will be discussed further.

Implications of AI on High-Tech Advancement

Official state data indicates that Chinese high-tech manufacturing experienced a 7.5% year-over-year added value increase in January and February of 2024, which combined with December 2023 data, "mark[ed] three consecutive months of accelerated growth" [12]. China's March 2024 "Two Sessions" convention, the major annual meeting of its two top political bodies, resulted in the announcement of an "AI Plus" initiative [13]. Notably, China explains that it focused its attention in the past on primarily developing AI technology, while now in 2024 it is shifting its attention to applications of AI [13]. While specific details remain unclear, this initiative signals a continued push in the AI space [13]. And while the announcement of a "Plus" initiative related to technology is not atypical given previous "Plus" initiatives such as last decade's "Internet Plus," it could be viewed as signaling lackluster AI advancement thus far [13]. Nonetheless, the Chinese Ministry of Industry and Information Technology announced that the initiative will be a key to furthering industrial and manufacturing upgrades and outputs, so time will tell how effective AI progress will be in facilitating that [12].

An "Ecosystems" View

Foreign Affairs asserts that the U.S. "is not yet competing on the same level" as China in the tech race [14]. The publication frames this race as two sided, in which U.S.-driven and China-driven realms are battling for dominance [14]. However, the authors of the piece argue that this is not a race between countries and/or companies, but rather between "technology ecosystems," global collaborative efforts between certain players [14]. Because of this, the U.S. must rally its allies including Germany, India, and South Korea to strengthen technology partnerships, build resilient supply chains, and increase technological adoption [14]. Coupled with strategic investments, the U.S. must seek to create the favorable conditions in which other countries are drawn to participate in its sphere of influence rather than China's [14].

Looking At the Road Ahead

While these good signs are clearly welcomed, the continuous goal for the U.S. has to be avoidance of being caught flat-footed. Unsurprisingly, the incorporation of AI into military capabilities is likely to increase U.S.-China rivalry and strategic risks [15]. Security experts advise that in addition to the U.S. taking clearer steps like limiting China's military AI development and advancing its own, as well as pursuing unilateral responsible military AI management policymaking, which it is already doing according to a senior DOD official, the U.S. should also pursue "bilateral and multilateral diplomacy to reduce strategic risks" [16, 15]. These experts suggest that the U.S. "take bold action" to hamper the progress China can make on its military AI by using narrowly tailored means that avoid self-harm [15]. Furthermore, they suggest that the U.S. prioritize intelligence gathering, analysis, and assessment regarding China's military AI capabilities [15, 17].

Revisiting the more qualitative, historical view, The Financial Times Editorial Board identifies "real risks" for the PRC's choices to prioritize "security, technology, and self-reliance over GDP growth" [18]. The Board also identifies "little evidence" that the country has spelled out policies capable of propelling it to reach its stated growth target [18]. The weaknesses China faces, including property issues, debts, deflation, and unemployment necessitate growth, and its focus on ideology over economics risks veering the country in the wrong direction [18].

The U.S. has a lot going for it in this area. That is a sentiment echoed by former Cyber Command leader General Nakasone in January 2024 testimony before the U.S. House Select Committee on the CPP. When asked by a Committee member whether America is winning the so-called cyber race, the General replied, "We are" [19]. The messages of analysts, experts, and scholars converge on and give rise to the broader idea that from both military and economic perspectives, the U.S. Department of Defense must look beyond the walls of the Pentagon and contribute to a more whole-of-government and whole-of-allied world approach involving interagency and international partners in order to succeed in taking preventative measures intended to stifle China's goal of proliferating AI while advancing its own AI interests.

<u>Internet of Things (IoT)</u>

The definition of IoTs by Oracle states 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, IoTs 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 IoTs Research and Development (R&D) including China and the U.S. In this paper, we will focus on the IoTs progress of these two countries.

Revenue and Investment by China and the U.S.

According to Statista 2022 report on IoTs total market, China has reached nearly 120 billion USD in revenue, and the revenue projection in 2025 will be around 205 billion USD. While the U.S. IoTs total market revenue in 2022 has reached 142.50 billion and is projected to be close to 225 billion USD in 2025. Additionally, the report on IoTs investment shows that China has invested 1.21 billion USD, while the U.S. has invested 1.45 billion USD. [3] As observation, the gap between the revenue of China and the U.S. is considerably narrowing down from 23.5 billion to 20.7 billion USD. This signals a fast growth of China economy in the next a few years in IoTs market alone, which China possibly catches up with the U.S. soon, even though the U.S. is also moving forward in this industry at a steady pace.

Top IoT Companies

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

Economic and High-Technology Aspects

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

Nevertheless, this dependency hints a cybersecurity problem that is created by those IoTs 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. In addition, there are roadblocks on the way of China

surpassing the U.S. One research shows that China is still on the go with its dispersed supply chain, various standards, and resistance to adopt industrial IoTs 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 to the IoTs playground, 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 IoTs businesses operate in China because of the low labor and land costs, therefore, the Chinese government seems to use regulations to restrict the growth of those businesses. In contrast, Chinese domestic IoTs business will receive heavy supports from the government to help the country improve its IoTs industry. One day it will set an advantage of China in global market. Besides national standards, China also attempts to influence international IoTs standards despite of past failures.

Current Challenges

One possible concern followed by China's expansion in IoTs global market is authorized and unauthorized access of IoTs devices or sensors that collect and possibly transfer users' data back to its manufacturing center. According to Smid, China proceeds in four ways to collect officially, which are via consent of consumers of its IoTs product, through devices' design phase, by obtaining foreign companies along with their data, and through Chinese government power that lets the government have a control over data collection. [9] Likewise, a vast entrance of Chinese IoTs products may pose a potential target to unauthorized access of a weak configuration that causes a secret data collection. Assuming that many U.S. citizens deploy China IoTs products with inadequate configurations, China may easily observe and collect both consumers' and national data.

One past report shows that "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] They alerted national security and were afraid of every image and video of states' activities will be sent back to Beijing when many American police departments and state governments adopt drones made by DJI, a private Chinese technology company.

Applications

From the IoTs 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] The author of this article also mentions how China may deploy IoTs military-based applications in which creating impact on military activities of foreign countries. In demonstration, one of popular wireless network trends is an unmanned aerial vehicle (UAV), which is mainly used by military to navigate automatically or remotely capture activities such as

troops' practices from the sky. These UAV is embedded with IoTs sensors or software that help connect to the network and transmit data efficiently. [12] However, it raises a concern of vulnerabilities such as Man-in-the-middle (MITD) that may gain unauthorized access to confidential systems and data. This would be a probable caution in the future since everything is now interconnected to the network.

Furthermore, China may be able to observe and record other countries' activities or even attack once it successfully tracks down its own system. Mr. Franz-Stefan Gady has been an advisor for many militaries in Europe and the U.S., as well as a conflict zone journalist. In 2021, he has created a fictional scenario on China and the U.S. Navy's technological capabilities over Taiwan in which mentioning Gongji-11 (GJ-11), along with claiming it was in testing and evaluating phases in Xinjiang province in the west of China. [13] This UAV was resembled American X-47B by its shape and size with an intense of an attack aircraft and stealth characteristics. In this approach, the aircraft is anticipated to enter its enemy territory and attack strategically important targets unnoticed. [14]

Together with the growth of 5G network that provides a faster and smoother connectivity for smart devices produced by China, it is likely to speed up the progress of taking over the IoTs dominant role. China seems to have a practically complete 5G national network, and with its large population, China will be able to collect more user data and potential vulnerability faster than before. As mentioned above, the three giant technology companies are holding a critical role in contributing to boosting national IoTs application, as well as building influences on international standards. To illustrate, Huawei is reported as an essential provider for 5G technology in most of 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 IoTs application. [15]

Additionally, AI development works side by side to enhance and manage the application of IoTs in China, especially in 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. [15] 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 IoTs standard setting.

Potential Solutions for the U.S.

Overall, the U.S. federal and state governments should quickly work toward solutions that help to mitigate the impact of those challenges above, 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 IoTs companies and products on entering a national market. For instance, the U.S. have recently done with TikTok that is owned by Byte Dance, a Chinese company. [15] 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 IoTs 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 a better IoTs improvement.

Aerospace Equipment

Aerospace is a term derived from two words: spaceflight and aeronautics. This aerospace industry deals with the manufacturing of aircraft and vehicular flights that occur beyond and within the Earth's atmosphere. This industry is also involved in the development, manufacture, and research. Some of the aircraft this industry manufactures are sailplanes and gliders, as well as military aircraft such as missiles and rockets. China has the leading and largest aerospace industry in the Asia-Pacific region, but as compared to the United States, it has limited capabilities.[1]

China has applied the aerospace equipment's in several sectors such as military, research and development, space exploration, and civil aviation. At the 18th Party Congress in 2012, the government members Li Keqiang, and Xi Jinping presented the 13th Five-Year Plan, in which they had the goal of turning communication and information technology into one of the highest priorities of China. The economy of China was pushed to higher values due to the plan of Made in China 2025. [5]

China's Investment

Aerospace equipment is one of the ten key sectors that are targeted by the Made in China 2025 plan. President Xi's military reforms established the PLASSF in 2015, which oversees the space-based military assets of China. China Aerospace Science and Industry Corporation (CASIC) has developed the space technology of the country.[6] The Chinese aerospace industry has started to become commercial. In 2017, investments were received by 17 Chinese aerospace enterprises. The investments were approximately 2.16 billion yuan, which is almost $308.6 million USD. Some private companies that are serving the development of the aerospace sector are iSpace, One Space, and China Rocket Co.[5]

China's Economy & Defense

China's aerospace sector has progressed a lot. It can emerge in direct competition with the USA in the global military and economic power by the year 2030. The ICBM (intercontinental ballistic missile) development in China has grasped 10% of the global market share due to its satellite launch capabilities. Also, there has been success in the sales of missiles. The economy of China has also been boosted due to the high demand for their aircraft, which has enabled the Chinese to do their production with less expertise and experience. Additionally, the aerospace industry has led to an increase in the industrial growth, job creation and technology development. [7]
China's defense industry has carried out several innovation activities due to guidance, and sustained support from the elites of the military and political leadership. A distinguishing characteristic of the defense system is that it runs an absorptive model of technology, such as an innovation-based system. Defense corporations have recorded higher annual profits. The

aerospace sector has engaged in the production of transport aircraft. On the other hand, there are conventional submarine programs, development, research, destroyers, surface warships, and four active nuclear programs initiated by the shipbuilding industry. The defense system of China has strengthened a lot since there were 60 vessels launched in 2014-2015, and 18 ships commissioned in 2016 including the 1 Types (052D DDG), and 3 Type (054A) guided missile frigates by the PLA Navy. The expenditure on China's development and research in 2015 was around 1.42 trillion, which is approximately $208 billion and 2.07 percent of the gross domestic product and this has been an increase of 8.9% since 2014. [8] According to Oliver Wymans's MRO international consulting firm, the travel market in China is expected to become one of the largest air travel markets in the world by the year 2030 since it is expected to reach $23.1 billion, which will result in 10.5% annual growth. [9]

U.S Investments

The aerospace industry of the U.S. consists of major companies like Northrop Gruman, Boeing, Textron, United Technologies, and Gulfstream along with some others. The established centers of aerospace manufacturing units are in Arizona, Kansas, California, Connecticut, and Texas. [3] A foreign direct investment of $21 billion has been in the aerospace sector of the U.S. at the end of the year 2019. [4]

The demand for space capacity has increased, which has, as a result, caused the U.S. to increase its spending in the aerospace industry. In 2022, the spending on aerospace programs increased by the government by up to 8%, according to the Space Foundation. Also, the United States Space Force (USSF) has requested more funding for the 2024 year. USSF has requested an amount of $30.1 billion, which is a result of a 15% increase as compared to the year 2023. Also to keep working on the International Space Station (ISS) research, and exploration of space to create economic and scientific opportunities there has been a budget request by NASA of $27.1 billion for the year 2024, which as compared to year 2023 has increased 7%. Likewise, 60% of the total budget has been allocated by the USSF for (RDT&E) such as research, development testing, and evaluation. [2]

U.S Economy & Defense

For the past 10 years, the top five export markets of the United States aerospace sector have been the same. The top market in 2011 was the United Kingdom, from 2012-2018 was China, and from 2010-2019 it was France. Except for the year 2012, Canada has also been among the top five markets for the last decade. The aerospace industry has the highest trade balance of 77.6 billion recorded in 2019, and the second highest level of exports of $148 billion. [10] This sector of the U.S. has increased employment. This industry has created a 2% national employment base. U.S. exports to different countries around $151 billion worth of goods and it has become one of the largest exporters in 2018. [11]

The budget for defense has increased by 3.18% year-over-year. The GDP of US defense is currently 3.1%. However, Due to increased inflation rates, there have been concerns raised among the defense authorities. [2] Even after suffering from a pandemic, this sector has boosted the U.S. economy, and the sales in the aerospace sector have contributed to 18.8% of the

revenue of the nation, and it accounts for 1.8% of the total U.S. GDP which is around $382 billion. [12]

Applications

In the U.S., AI has been very effective in simplifying the aircraft's design. It helps enhance the manufacturing process and automate quality control. Also, artificial intelligence enables the detection of defects that are present in the components, and it results in increased efficiency. Artificial intelligence has improved air traffic management, and it is playing an important role in space exploration expansion and satellite systems. AI is helping to improve fuel efficiency, inspection processes, and repairs in military aircraft. The algorithms that are created by AI which include data on the fly can help aircraft choose a route that is less risky and more stable to avoid weather conditions and accidents. It also helps the engineers in aerospace sector to utilize feature recognition and deep learning to extract the values from the data and then use it to explore designs with more efficiency. [13]

China has set new goals to use AI to transform its military technological development from mechanization to information to intelligentization, such as integrating artificial intelligence, quantum computing, and other emerging technologies into a joint force by the year 2027. According to the researchers at the Center for Security and Emerging Technology, the seven areas of interest in which AI is being used are 1) information and electronic warfare, 2) intelligent and autonomous vehicles; 3) simulation and training, 4) intelligence and surveillance; 5) automated target recognition; 6) predictive maintenance and logistics, and 7) command and control. Artificial intelligence has enabled the operation of autonomous vehicles, such as drones, on air, ground, subsea, and sea surfaces without an onboard crew. [14]

Challenges

One of the biggest challenges for the aerospace industry is the cybersecurity threat. The issue is that companies in this sector have high-value data and assets which is a particular target for cybercriminals. Another challenge in this industry is the disruption of the supply chain. The disruption causes delays in shipping, compliance issues, material shortage, and rising cost of supplies. [15]

On the other hand, another event of challenge in this sector is the crash of the F-35 fighter jet while landing at Hill Air Force Base Utah on 19 October 2022 after returning from training. The crash occurred due to a glitch that occurred in the computer system of the jet due to turbulence. The aircraft was not resilient and robust towards external environmental factors. In other words, the Air Data System is used to collect information from external sensors from both the right and left sides of the aircraft, and in return, it helps the aircraft computer in making precise control adjustments. However, due to turbulence it experienced disruptions and led to inaccurate information being used by the computer for control adjustment resulting in a crash. [16]

Recommendations

As we can see, the United States is still ahead of the world and China in aerospace and many other fields. But China is very close to closing this gap due to its technologies, skills, hard work, and expertise. Hence, it is very important that the United States invests more in technology establish more research programs and employ more talented people to enhance their work in the aerospace sector. The People's Liberation Army Air Force (PLAAF), and the PLA Rocket Force (PLARF) have surpassed U.S. military capabilities.

China has built a long-range strike missile force, which includes ballistic missiles of various ranges. They have built anti-access and area denial (A2/AD) capability, which is a challenging aspect for the U.S. to freely operate in certain regions. China has also built hypersonic weapons such as the DF-17, which travel a high speed and are difficult to defend against. Another thing is that PLAAF has more advanced and larger grounds as compared to the U.S. for air and missile defense systems. The U.S. needs to focus on developing hypersonic systems in the Navy, Army, and Air Force. It also needs to enhance its missile defense to intercept missile threats by updating its existing systems such as Patriot SAM. Also, support the initiatives to support the growth of drones. [17]

Author Statement

This project was a chance for our team to work closely with a real client, U.S. Cyber Command where we conducted research based on our client's perspective and feedback. We also received weekly feedback and guidance from our Professor, Brian Ngac. Team meetings helped us to keep track of one another's progress, exchange information and feedback from one another and work on our execution plan as well. The presentation with our client was a new experience for us as we delivered our final findings and potential solutions/recommendations to our client. In addition, we learned how to adjust our schedule and communicated regularly with our clients to meet their needs. In general, this project was a new experience for all of the team members.

References

Introduction

1. U.S. Department of Defense, "2022 National Defense Strategy," 27 October 2022, https://media.defense.gov/2022/Oct/27/2003103845/-1/-1/1/2022-NATIONAL-DEFENSE-STRATEGY-NPR-MDR.PDF
2. McBride, J.; A. Chatzky; "Is 'Made in China 2025' a Threat to Global Trade?," Council on Foreign Relations, 13 May 2019, https://www.cfr.org/backgrounder/made-china-2025-threat-global-trade
3. U.S. Office of the Director of National Intelligence, "Annual Threat Assessment of the U.S. Intelligence Community," 5 February 2024, https://www.dni.gov/files/ODNI/documents/assessments/ATA-2024-Unclassified-Report.pdf

Quantum Computing

4. Penney, H. R. (2024, March 22). The Quantum Advantage: Why It Matters and Essential Next Steps. Mitchell Institute for Aerospace Studies. https://mitchellaerospacepower.org/the-quantum-advantage-why-it-matters-and-essential-next-steps/
5. Bogobowicz, M., Gao, S., Masiowski, M., Mohr, N., Soller, H., Zemmel, R., & Zesko, M. (2023, April 24). Quantum Technology sees record investments, progress on talent gap. McKinsey & Company. https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/quantum-technology-sees-record-investments-progress-on-talent-gap
6. Freedberg, S. J. (2024, March 4). China's investing billions in quantum R&D, but is Beijing making some bad bets? Breaking Defense. https://breakingdefense.com/2024/02/chinas-investing-billions-in-quantum-rd-but-is-beijing-making-some-bad-bets/
7. Dargan, J. (2021, April 20). 9 Chinese Quantum Computing Companies Leading the National Race. The Quantum Insider. https://thequantuminsider.com/2021/04/20/9-companies-leading-the-quantum-technologies-race-in-china/
8. Klebanov, S. (2022b, February 23). *Who's winning the quantum computing race? China and the U.S. are neck and neck*. The Business of Business. https://www.businessofbusiness.com/articles/whos-winning-the-quantum-computing-race-china-and-the-us-are-neck-and-neck/
9. Pichai, S. (2019, October 23). *What our quantum computing milestone means*. Google. https://blog.google/technology/ai/what-our-quantum-computing-milestone-means/
10. Smith-Goodson, P. (2019, October 11). *Quantum USA vs. Quantum China: The world's most important technology race*. Forbes. https://www.forbes.com/sites/moorinsights/2019/10/10/quantum-usa-vs-quantum-china-the-worlds-most-important-technology-race/?sh=37cd43fd72de
11. Amerongen, M. van. (2021, June 3). Quantum Technologies in Defense & Security. NATO Review. https://www.nato.int/docu/review/articles/2021/06/03/quantum-technologies-in-defence-security/index.html
12. Shams, M., Choudhari, J., Reyes, K., Prentzas, S., Gapizov, A., Shehryar, A., Affaf, M., Grezenko, H., Gasim, R. W., Mohsin, S. N., Rehman, A., & Rehman, S. (2023). The

Quantum-Medical Nexus: Understanding the Impact of Quantum Technologies on Healthcare. Cureus, 15(10), e48077. https://doi.org/10.7759/cureus.48077

13. Swayne, M. (2024, February 28). Reports: China mass producing dilution refrigerator critical to superconducting quantum computing. The Quantum Insider. https://thequantuminsider.com/2024/02/28/reports-china-mass-producing-dilution-refrigerator-critical-to-superconducting-quantum-computing/#:~:text=REQUEST%20ACCESS-,QUANTUM%20TECHNOLOGY%20IN%20CHINA,-Our%20Quantum%20Technology
14. Toon, J., (2024, February 6). New ion cooling technique could simplify quantum computing devices. Phys.org. https://phys.org/news/2024-02-ion-cooling-technique-quantum-devices.html#:~:text=Using%20a%20technique%20called%20rapid%20ion%20exchange%20cooling%2C
15. Williams, L. (2021, November 9). The world's top five quantum computing hubs. Investment Monitor. https://www.investmentmonitor.ai/tech/the-worlds-top-five-quantum-computing-hubs/?cf-view&cf-closed
16. Precedence Research. (2023, January 30). Medical Tourism Market Size to Surpass USD 286.1 Bn by 2030. Www.precedenceresearch.com. https://www.precedenceresearch.com/medical-tourism-market
17. Liu, N. (2024, February 16). China invests billions in quantum computing, race with US now neck-and-neck. SDxCentral. https://www.sdxcentral.com/articles/analysis/china-invests-billions-in-quantum-computing-race-with-us-now-neck-and-neck/2024/02
18. NIST. (2023, August 24). NIST to standardize encryption algorithms that can resist attack by quantum computers. The National Institute of Standards and Technology. https://www.nist.gov/news-events/news/2023/08/nist-standardize-encryption-algorithms-can-resist-attack-quantum-computers
19. Sanzeri, S. (2023, February 6). The quantum threat: Our government knows more than you do - cyber ... Cyber Defense Magazine. https://www.cyberdefensemagazine.com/the-quantum-threat-our-government-knows-more-than-you-do/
20. Kitchen, K., & Drexel, B. (2021, April 22). Quantum Computing: A National Security Primer. American Enterprise Institute - AEI. https://www.aei.org/research-products/report/quantum-computing-a-national-security-primer/
21. Dargan, J. (2024, February 17). Quantum Computing Companies: A full 2024 list. The Quantum Insider. https://thequantuminsider.com/2023/12/29/quantum-computing-companies/#:~:text=Contact%20Us%20page-,Quantum%20Computing%20in%20Modern%20Industries,avenues%20for%20tackling%20computational%20challenges

AI/ML

4. U.S. Bank, "Analysis: China's economy and its influence on global markets," 4 April 2024, *https://www.usbank.com/investing/financial-perspectives/market-news/chinas-economic-*

influence.html#:~:text=China's%20economic%20reopening%20and%20growth,considered%20lagging%20by%20historical%20standards

5. Branstetter, L.; G. Li; "The actual effect of China's 'Made in China 2025' initiative may have been overestimated," Centre for Economic Policy Research, 11 August 2023, *https://cepr.org/voxeu/columns/actual-effect-chinas-made-china-2025-initiative-may-have-been-overestimated*
6. Allen, G. C.; "China Is Striking Back in the Tech War With the U.S.," Time, 20 July 2023, *https://time.com/6295902/china-tech-war-u-s/*
7. Allen, G. C.; "Advanced Technology: Examining Threats to National Security," Center for Strategic and International Studies, 19 September 2023, *https://www.csis.org/analysis/advanced-technology-examining-threats-national-security*
8. DeSmith, C.; "Why China has edge on AI, what ancient emperors tell us about Xi Jingping," The Harvard Gazette, 16 March 2023, *https://news.harvard.edu/gazette/story/2023/03/why-china-has-an-edge-on-artificial-intelligence/*
9. Citi, "China AI: What Lies Ahead?," 4 April 2023, *https://www.citigroup.com/global/insights/global-insights/china-ai-what-lies-ahead*
10. Mozur, P.; J. Liu; C. Metz; "China's Rush to Dominate A.I. Comes With a Twist: It Depends on U.S. Technology," The New York Times, 28 February 2024, *https://www.nytimes.com/2024/02/21/technology/china-united-states-artificial-intelligence.html#:~:text=As%20much%20as%2050%20percent,jumped%20into%20the%20generative%20A.I*.
11. Sheehan, M.; "China's AI Regulations and How They Get Made," Carnegie Endowment for International Peace, 1 July 2023, *http://www.jstor.org/stable/resrep52039*
12. Global Times, "China to accelerate AI innovation to empower high-tech manufacturing: MIIT," 26 March 2024, *https://www.ecns.cn/news/economy/2024-03-27/detail-ihcyyfhe2565761.shtml*
13. Xu, Y.; D. Castro; "What's Next After the Two Sessions for AI in China," Center for Data Innovation, 25 March 2024, *https://datainnovation.org/2024/03/whats-next-after-the-two-sessions-for-ai-in-china/*
14. Thomas, C.; S. Kreps; "America Can't Win the Tech Race Alone," Foreign Affairs, 26 January 2024, *https://www.foreignaffairs.com/united-states/america-cant-win-tech-race-alone*
15. Stokes, J.; A. Sullivan; N. Greene; "U.S.-China Competition and Military AI: How Washington Can Manage Strategic Risks amid Rivalry with Beijing," Center for a New American Security, 1 July 2023, *http://www.jstor.org/stable/resrep52263*
16. Horowitz, M. C.; G. C. Allen; "The State of DOD AI and Autonomy Policy," Center for Strategic and International Studies, 9 January 2024, *https://www.csis.org/events/state-dod-ai-and-autonomy-policy*
17. Webster, G.; R. Hass; "A roadmap for a US-China AI dialogue," Brookings Institution, 10 January 2024, *https://www.brookings.edu/articles/a-roadmap-for-a-us-china-ai-dialogue/*

18. The Editorial Board; "China lacks a credible policy to meet its own growth target," Financial Times, 6 March 2024, *https://www.ft.com/content/9e2b59be-1f06-4001-bf68-91974951ec59*
19. Nakasone, P.; R. Torres; "The CCP Cyber Threat to the American Homeland and National Security," U.S. House of Representatives Select Committee on the Strategic Competition Between the United States and Chinese Communist Party, 31 January 2024, *https://selectcommitteeontheccp.house.gov/sites/evo-subsites/selectcommitteeontheccp.house.gov/files/evo-media-document/1.31.24%20Hearing%20Transcript.pdf*

IoT

1. McBride, J., and 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 (**** Used in Introduction of individual paper)
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. Gady, F.-S. (2021, June 9). *How Chinese unmanned platforms could degrade Taiwan's air defense ...* IISS. https://www.iiss.org/blogs/analysis/2021/06/china-taiwan-unmanned-platforms
14. Military Factory. (2019). *Gongji-11 (GJ-11)*. Gongji-11 (GJ-11) Stealth Unmanned Combat Aerial Vehicle (UCAV). https://www.militaryfactory.com/aircraft/detail.php?aircraft_id=2219
15. Fowle, H. (2023, December 7). *IOTS's china conundrum*. IOTS Insider. https://www.IoTsinsider.com/news/analysing-chinas-ascendancy-in-the-IoTs-landscape/
16. 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

Aerospace Equipment

1. Amir, A. R., & Weiss, S. I. (2024, January 8). *Aerospace industry*. Encyclopedia Britannica. https://www.britannica.com/technology/aerospace-industry
2. Berckman, L., Hardin, K., Sloane, M., & Dronamraju, T. (2023, November 29). *2024 aerospace and Defense Industry Outlook*. Deloitte Insights. https://www2.deloitte.com/us/en/insights/industry/aerospace-defense/aerospace-and-defense-industry-outlook.html
3. Michaela, P. (2009b, December 3). *U.S. Aerospace Manufacturing: Industry Overview and Prospects*. EveryCRSReport.com.https://www.everycrsreport.com/reports/R40967.html
4. *Selectusa Aerospace Industry*. International Trade Administration | Trade.gov. (2021b). https://www.trade.gov/selectusa-aerospace-industry
5. Sinha, R. (2019, November 5). *The rise of the Chinese Aerospace Sector - prescouter - custom intelligence from a global network of experts*. PreScouter. https://www.prescouter.com/2019/11/rising-chinese-aerospace-sector/
6. Nouwens, M., & Legarda, H. (2018, December 18). *China's pursuit of dual-use technologies*. IISS. https://www.iiss.org/research-paper//2018/12/emerging-technology-dominance
7. Erickson, A. (2020). *China's aerospace development and its larger implications*. East West Center. https://www.eastwestcenter.org/sites/default/files/private/IGSCwp003.pdf
8. Cheung, T. M. (2017, March 1). *Strengths and weaknesses of China's Defense Industry and acquisition system and implications for the United States*. Calhoun Home. https://calhoun.nps.edu/handle/10945/58878
9. *China - aviation*. International Trade Administration | Trade.gov. (2023, April). https://www.trade.gov/country-commercial-guides/china-aviation
10. *Leading Economic Indicators Aerospace Industry*. International Trade Administration | Trade.gov. (2023). https://www.trade.gov/leading-economic-indicators-aerospace-industry#:~:text=Overview,billion)%20among%20all%20manufacturing%20industries.

11. Pulskamp, A. (2023a, November 29). *The impact of the aerospace industry in the USA economy*. The Impact of the Aerospace Industry in the USA Economy. https://blog.brennaninc.com/the-impact-of-aerospace-and-defense-on-the-us-economy
12. *2021 facts & figures: U.S. Aerospace & Defense*. 2021 Facts & Figures: U.S. Aerospace & Defense Industry. (2021, September 15). https://facts.aia-aerospace.org/
13. Patil, A. (2023, September). *The good, the bad, and the awful of AI in aerospace*. Aerospacemanufacturinganddesign.com. https://www.aerospacemanufacturinganddesign.com/news/the-good-the-bad-and-the-awful-of-ai-in-aerospace-most-read-2023/
14. Strokes, J. (2024b, February 1). *Military Artificial Intelligence, the People's Liberation Army, and u.s.-china strategic competition*. Center for a New American Security (en-US). https://www.cnas.org/publications/congressional-testimony/military-artificial-intelligence-the-peoples-liberation-army-and-u-s-china-strategic-competition
15. *Top 5 challenges in the aerospace industry*. Top 5 Challenges in the Aerospace Industry | CP Cases. (2023b). https://cpcases.com/us/news/top-5-challenges-in-the-aerospace-industry
16. Roza, D. (2023, July 31). *F-35 crashed due to computer glitch caused by turbulence: Accident report*. Air & Space Forces Magazine. https://www.airandspaceforces.com/air-force-f-35-crash-hill-report/
17. Ohlandt, C. (2023, April 13). *U.S.-China Aviation Competition Military, Commercial, and General Aviation Are Different.* Rand Coporation. https://www.rand.org/content/dam/rand/pubs/testimonies/CTA2600/CTA2692-1/RAND_CTA2692-1.pdf