CENTRE FOR STRATEGIC AND CONTEMPORARY RESEARCH

CSCR

Perspectives
Issue No. 28

01 October 2021

Data, not Arms: New Frontier in US-China Geopolitics

Author: Rida Fatima*

Key Points:

- The "Geopolitics of Information" has shifted the centre of the oft-repeated yet conflicted question regarding who will shape the global political economy, and how.
- Information is now the most valuable and contentious geopolitical resource on the planet. Data is likely the "new oil".
- In essence, information power is transforming the nature and behaviour of state, which is the foundation of international relations with potentially seismic implications.
- The ubiquity of data and artificial intelligence (AI) will transform diplomacy by increasing both the number of non-governmental actors who influence formal diplomacy and the purposes for which that data is employed.
- The US government sees itself in a tech arms race with the Chinese government. The US recognises the transformative role of new technologies in national security.
- The most interesting conflict ahead is not between China and the United States (US). It is between business elites in both nations who are seeking big profits, and the political elites on both sides who want to protect their countries, and so doing, their own centres of power.

Information is now the most valuable and contentious geopolitical resource on the planet. For years, the world's most profitable companies have claimed that data is the "new oil."[1] In essence, the power of information is transforming the nature and behaviour of state, which is the foundation of international relations with potentially seismic implications. The "Geopolitics of Information" has shifted the centre of the oft-repeated conflicted question as to who will shape the global political economy, and how. The distribution of the world's communication networks, and information resources is a sector of social contestation, involving a broader set of social actors, as well as a realm of political-economic rivalry between nations and companies.

In recent times, the emerging tussle between Washington and Beijing can also be analysed in the same context. Arguably, the emerging cold war between the two powers tends to fall in the domain of "information power struggle", and power of this data lies in collecting, synthesising, and analysing information to outmaneuvre the opposition.

China has long been accused of stealing American technology by successive US governments. The Trump administration has upped the accusations by requesting that Huawei, China's largest technology company, be placed on an international blacklist, accusing it of being a cover for China's ambitions to infiltrate other countries' telecommunications infrastructure for strategic gain. During the Biden administration, numerous incidents of charges have occurred in a similar manner. Nonetheless, the Chinese rhetoric in this regard has taken an aggressive shape. This is reflected in Beijing's increasingly forward-

[1] Philipp Hartmann and Henkel Joachim, "Really the new oil?'' a resource-based perspective on data-driven innovation." *Academy of Management Global Proceedings* (2018): 142.

* Rida Fatima is a graduate of the School of Politics and International Relations, Quaid -I- Azam University. She serves as a Research Assistant at the Centre for Strategic and Contemporary Research.

leaning information warfare approach. It's part of China's "Wolf Warrior Diplomacy'', which began in 2020 after Chinese Foreign Minister Wang Yi directed his country's envoys to be more forceful in expressing Beijing's interests abroad and loud in defending the Chinese Communist leadership.[2]

All Information is Strategic

The most important fight going on right now is a quieter kind of conflict - the combatants of Cold War 2.0 are squabbling over the modern era's currency: data. The ubiquity of data and artificial intelligence (AI) will redefine diplomacy by increasing the number of non-governmental actors who affect formal diplomacy as well as the goals for which data is used.[3]

Initially, the geopolitical significance of data and information was highlighted in 1998 by Robert Keohane and Joseph Nye. They classified information into three categories: free, commercial, and strategic. They characterised free information as personal information that people voluntarily shared online, whereas commercial information, such as intellectual property (IP), was only useful to corporations. Only one type of information was designated as "strategic information'', such as state secrets that would be of interest to governments and relevant to world events.[4] As the field of geopolitics expands, this distinction is becoming increasingly hazy. Every piece of information in this new era has the potential to be strategic. Data is at the center of the new wars.

This area of strategic tussle and vulnerability is much more feasible for states as it has a low entry cost, blurred traditional combat boundaries, the use of perception management and more. This creates a level-playing field, at least for those who are developing their expertise in this sector.[5]

China's AI Boom

In the new era, the data at one pole will impact people, politics, and businesses on the other pole of the world. It all boils down to who has more information on the other and can use it the most effectively in terms of cybersecurity. According to a study published by ITIF's (Information Technology and Innovation Foundation) Centre for Data Innovation, the United States is losing momentum to China in the AI race. According to the National Security Commission on AI (NSCAI), the United States government is "far from AI-ready", warning that "America's technological predominance is under jeopardy for the first time since World War II."[6]

The US has long been at the forefront of AI research, with premier universities and top people. However, it is in danger of relinquishing leadership to the Asian Tiger, which would have far-reaching consequences. Meanwhile, China, which stated its intention to dominate the global AI market by 2030, is rapidly gaining ground by increasing its investment in AI research. It's developing an advanced guard in a fight that will determine economic primacy in the Big Data era.

The AI growth in China has fuelled the country's growing confidence in its growing technological foundation. President Xi Jinping has declared AI as one of the core pillars of the Made in China 2025 economic transformation plan.

At the same time, China's growth is instilling in the US a fear that its technological superiority is no longer intact. At least in part, the Trump administration's plans for a trade war with China remain motivated by concerns about China's technological progress. According to one Google official, last year's Go match, in which a system developed by Google subsidiary DeepMind defeated premier player Ke Jie in an ancient Chinese board game, was China's AI wake-up call. The US only realised how far they had come when the Russians launched Sputnik, while China had that moment when they lost at AlphaGo.[7]

Furthermore, statistics on the output of China's research institutions are rapidly increasing. In terms of the second type of hardware development, China has been slower to build the sort of homegrown chip industry needed to put it on the leading edge. This is owing in part to a series of judgments that effectively prohibit the acquisition of US semiconductor businesses, which began under President Barack Obama and increased under President Donald Trump.[8] Most experts believe China's AI advantage lies in the last element, the availability of raw data.

[2] Zhiqun Zhu, "Interpreting China's 'Wolf-Warrior Diplomacy'", *The Diplomat*, May 2020.

[3] Gregory F. Treverton and Pari Esfandiari, "Data Governance and Geopolitics", *CSIS,* January 2021.

[4] Robert O Keohane and Joseph S. Nye, ''Power and Interdependence in the Information Age'', *Foreign Affairs*, 77(5), September/October 1998.

[5] Molander, Roger C., Andrew Riddile, Peter A. Wilson, and Stephanie Williamson, *Strategic information warfare: A new face of war*. Rand Corporation, 1996.

[6] Amy Borrett," The US is losing ground to China in the Global Race for AI Leadership", *Tech Monitor,* March 2021.

[7] Huw Roberts, Josh Cowls, Jessica Morley, Mariarosaria Taddeo, Vincent Wang, and Luciano Floridi. "The Chinese approach to artificial intelligence: an analysis of policy, ethics, and regulation." *AI & SOCIETY* 36, no. 1 (2021): 59-77.

[8] Paul Mozur, "Google's AlphaGo defeats Chinese Go Master in win for AI." *The New York Times*, May 2017.

[9] Gregory C. Allen, *Understanding China's AI strategy: Clues to Chinese strategic thinking on artificial intelligence and national security*. Washington, DC: Center for a New American Security, 2019.

The Rising threat Perception

The broader idea that allowing China to join the global economy would make it a "responsible partner" and lead to political reform, did not turn out to be the case. Joe Biden, on the other hand, is turning Trump's bombast into a philosophy pitting the US against China, a war between competing political systems with only one winner, according to him. This seems to mark the more dramatic break in American foreign policy in the five decades since Richard Nixon went to China.

It is clear that the US government considers itself to be in a technological arms race with China. The US believes that these technologies are so transformational that a country that takes the lead will benefit not only economically and technologically, but also in terms of national security.

Besides, the states can obtain the global data from a variety of sources and through a variety of methods. Malicious cyber intrusions are one apparent source. The Microsoft Exchange breach, which was purportedly carried out by Chinese security authorities, is a recent example.[9] However, data can be sourced from less visible and more standardised data collection methods that take use of authorised downstream data access via digital supply chains. The Pegasus spyware, for example, was discovered to target data from the phones of "lawyers, human rights defenders, religious figures, academics, businesspeople, diplomats, senior government officials, and heads of state", demonstrating how data (such as location data) can enable the surveillance of specific individuals.[10] However, it still targets a still-relatively small set of people. This is very strategic data which the state elites can utilise as a springboard for their next big move.

Earlier in 2021, Didi, China's largest ride-hailing app, saw its stock plummet by more than 20%. Didi had previously raised $4.4 billion in a major IPO (initial public offering) in New York, which was the largest IPO by a Chinese firm since Alibaba's launch in 2014.[11] The declaration by China's Cyberspace Administration that Didi was suspected of illegally gathering and utilising personal information was the immediate cause of Didi's demise. It had ordered Didi to halt registering new customers while it conducted an inquiry and had removed Didi's app from China's app shops.

Didi, according to China's state-owned *Global Times,* has the "most thorough personal travel information" of all global internet companies, and poses a possible risk to individuals since it can undertake big data analysis of customers' patterns and behaviour.

More likely, Beijing was concerned that the big IPO in New York would give the US access to vast amounts of personal data about where the Chinese people live, work, and travel — data that could jeopardise China's national security. Several internet companies, including Didi, were penalised by China's antitrust authority for allegedly breaking the country's anti-monopoly statute.[12] Politicians in Washington are almost as concerned as their counterparts in Beijing about intelligence leaks to the opposing side.

The Janus-Faced Threat in Making

Data security fears in Beijing and Washington are understandable. In practice, though, the two economies are inextricably linked. China's economy is still officially state-run and communist. Unofficially, its high-tech tycoons are as capitalist as their American counterparts–and have become almost as wealthy.

Entrepreneurs and financial geniuses in both China and the US are fully aware that the two countries together represent the world's largest market. Regardless of their individual politicians' increasing techno-nationalism, they will continue to do whatever they can to profit from this massive market. As a result, the most exciting battle to come is not between China and the US. It is a battle between economic elites in both countries looking for enormous profits and political elites in both countries looking to safeguard their governments and, as a result, their own centres of power. In the future, this data will undoubtedly reshape state-to-state ties.

Conclusion

Data security fears in Beijing and Washington are understandable. In practice, though, the two economies are inextricably linked. China's economy is still officially state-run and communist. Unofficially, its high-tech tycoons are as capitalist as their American counterparts, and have become almost as wealthy.

Entrepreneurs and financial geniuses in both China and the US are fully aware that the two countries together represent the world's largest market. Regardless of their individual politicians' increasing techno-nationalism, they will continue to do whatever they can to profit from this massive market. As a result, the most exciting battle to come is not between China and the US. It is

[10] Stephan Dziedzic, 'China was blamed for the Microsoft Exchange hack, but the consequences might end there,' *ABC News,* July 2021.

[11] Paul Lewis, "Huge data leak shatters the lie that the innocent need not fear surveillance," *The Guardian,* July 2021.

[12] Robert Reich, "War not Arms, the key driver in US-China emerging Cold War", *The Guardian,* July 10, 2021.

[13] 'China regulator fined internet platforms including Didi for illegal merger deals,' *Reuters*, July 7, 2021.

a battle between economic elites in both countries looking for enormous profits and political elites in both countries looking to safeguard their governments and, as a result, their own centres of power. In the future, this data will undoubtedly reshape state-to-state ties.

Recommendations

The issues facing this new front of battle are numerous, and despite growing attention, the present policy debate surrounding these information campaigns lacks clear—and necessary—long-term goals. To prevent the dangers from spiraling out of control, the following precautionary steps can be taken.

• The two countries should approach information warfare as any other major threat to global security. Disinformation mitigation, such as eliminating questionable inorganic accounts and posts, can never be fast enough to put malicious malware and data theft at bay.

• Along these lines, state and civil society governments should take a step back and focus on the entire ecosystem of information warfare, including where it originates from, how it is used, and what impact it has on global security.

• Security stakeholders should expect this phenomenon to become the new normal of political and economic life, requiring a holistic global response.

• The current data regulatory framework is muddled and complex. The only way to safeguard its national security component is for it to become a part of both sides of the Atlantic's defence strategy. The states may deploy a joined-up strategy against the connected threats we face.