AWM The Andrew W. Marshall
FOUNDATION

The Andrew W. Marshall Papers

“A State in Disguise of a Merchant”

Multinational Tech Corporations and the Reconfiguration of the Balance of Power in Asia

TRESTON WHEAT

Winner of the Inaugural Andrew W. Marshall Paper Prize on Future Reconfigurations in Asia

Foreword

What might the character of Asia be over the coming decades? How might Asia be restructured internally and interact with the rest of the world in new ways? What could drive those changes, and what could the consequences be?

Throughout his life, Andrew Marshall was interested in broad changes in the competitive environment. Beginning with his interest in Arnold Toynbee's *A Study of History*, he endeavored to understand the circumstances in which these changes occurred, such as new actors or regions rising to prominence while others dissipated and the character of the social, cultural, and other dynamics around such shifts. Marshall spent his early career at the RAND Corporation, where he and other prominent strategists considered these major shifts while developing and maturing methods of analyzing the nature of long-term competitions.

As director of the Office of Net Assessment in the Department of Defense, Marshall began opining that that a broad change might be taking shape. As part of his participation in the Commission for Long-Term Integrated Strategy, he and Charles Wolf directed a study of the future security environment. Completed in 1988, the study concluded that observable economic trends could reshape the world by making Asia—not Europe and North America—the economic center of gravity of the world. Though many found this thesis fanciful, Marshall continued to sponsor research to understand the ways in which the countries of Asia might develop as economic and military powers and the concomitant paths along which the Asia-Pacific region more generally might evolve.

Marshall was also interested in how Asia itself might develop new internal structures and institutions. Describing how the maps of Europe and China had changed from 1900 to 2000, he encouraged analysts to consider how the map of the Asia-Pacific might change by 2050 and which dynamics might drive those changes. Borders might change. Patterns of interactions within Asia might change. He encouraged cross-disciplinary work to understand these changes, chronicle their histories, and explore their trajectories in order to make informed forecasts for the United States about possible shapes of the region in the decades to come.

"A State in Disguise of a Merchant: Multinational Tech Corporations and the Reconfiguration of the Balance of Power in Asia," by Treston Wheat, the grand prize winner of the inaugural Andrew W. Marshall Paper Prize on Future Reconfigurations in Asia, is a thought-provoking survey of the modern rise of tech corporations and their impact on how states interact with each other and achieve their strategic objectives. The reconfiguration explored in this paper is one of power. It raises new questions, not only about Asia but also about the rest of the world. We are proud to present this paper, which identifies topics of strategic significance and takes an original approach by applying the lens of a cyber expert to regional dynamics.

The Andrew W. Marshall Foundation
October 2022

About the Author

Treston Wheat

Winner of the Andrew W. Marshall Paper Prize on Future Reconfigurations in Asia

Treston Wheat is a red team analyst with Milestone Technologies focusing on threat actor/tactics, techniques, and procedures research; wargaming; and alternative analysis. He is also an adjunct professor at Georgetown University. Previously, he worked as a strategic cybersecurity analyst and geopolitical risk analyst for AS Solution embedded in a major tech company. He received his Ph.D. from the University of Tennessee, Knoxville (UTK) with a dissertation on Augustinian just war theory and drone warfare, and during that time taught classes on American government, the presidency, and political cinema. He also received his B.A. in Political Science and History from UTK and his M.A. in Security Studies from Georgetown University.

Table of Contents

When corporations were created four centuries ago, they fundamentally altered the relationship between the market and the state while also shifting geopolitical power. Technology corporations are creating a similar revolution in the contemporary age. As the world moves from industrial and postindustrial economies to digital ones, technology companies now touch practically every area of modern life. Politically and geopolitically, they are also changing how states interact with each other and achieve their strategic objectives. Technology corporations now play a central role in states' relative power, and over the next two decades they will impact the balance of power in Asia. A country's relative power may be intimately connected to native technology companies as they become essential to economic growth, defend infrastructure and businesses, participate in investigations and attributions of cyber events, and even engage in offensive cyber operations. This paper looks at those different areas, examines trends, and then posits a plausible future in which technology corporations may contribute to a reconfiguration of the balance of power in Asia by 2045.

Introduction

During the heyday of modern empires, corporations played a significant role in advancing the values, economies, and interests of the countries in which they were based. Corporations were efficient mechanisms for accumulating wealth from foreign lands, but to do so they often had to wield hard power through mercenaries or direct relationships with the military. The East India Company behaved as a territorial power from the 1760s until the revocation of most of its commercial functions in the 1830s, so much so that Edmund Burke in the 1780's commented during a parliamentary impeachment that it acted as a "state in disguise of a merchant."[1] While today's multinational technology companies do not have the same kind of direct hard power, they do wield an incredible and equivalent amount of sociopolitical and economic power. Technology companies play a much larger role than any other economic sector in modern daily life, from financial transactions to agricultural production to automobiles to warfighting. Most importantly, multinational technology companies play a vital role in the new fifth domain, becoming both targets of cyberattacks and producers of them.[2] Governments are no longer the only or even the primary targets of sophisticated intelligence collection or cyberattacks: corporations fall within the geopolitical battlespace.

This role extends to warfare, including artificial intelligence, intelligence analysis, cyberattacks and cyber defense, espionage, critical infrastructure, mercenary technology, and protecting personal data. To better understand this trend of corporations taking on a security role and its impact on geopolitics, this paper looks at the role of multinational corporations in the reconfiguration of Asia, where the balance of power is changing because of technology firms' pervasiveness and the role of technology in national security. Balance of power refers to the relative power between countries; it indicates the possible threats they pose to each other and the influence they wield. Power in international relations is derived from a country's economic strength and ability to project force. Shifts in this balance can lead to conflict, while maintaining a status quo can create stability.[3] The reconfiguration of power in Asia

[1] Julie Murray, "Company Rules: Burke, Hastings, and the Specter of the Modern Liberal State," *Eighteenth-Century Studies* 41, no. 1 (Fall 2007): 56.

[2] Cyber is the fifth, and newest, domain of warfare. The first four are land, sea, air, and space. Cyber is a broad category as a domain, and it includes everything from computers to telecommunications networks to fiber-optic cables to digital data to the internet of things and more.

[3] Hal Brands and Michael Beckley, "China Is a Declining Power—And That's the Problem," *Foreign Policy*, September 24, 2021, https://foreignpolicy.com/2021/09/24/china-great-power-united-states/. See also Graham Allison, *Destined for War: Can America and China Escape the Thucydides Trap?* (Boston: Houghton Mifflin Harcourt, 2018); Henry Kissinger, *A World Restored: Metternich, Castlereagh, and the Problems of Peace 1812-1822* (Boston: Houghton Mifflin Company, 1957), 6.

over the next few decades will depend on the role multinational tech corporations play and how they are directly engaging with the core state function of security, both in concert with states and independently.

The first part of this paper sets the stage by exploring a state's core functions and looking at historical examples of private entities taking on these functions. The next section provides examples of the role of technology and technology companies in the core state function of security. To illustrate these broader trends and explore how multinational tech corporations may take on increasingly greater roles, the paper examines the role of China and how its tech corporations are taking on covert operations, the impact of the balkanization of the internet and economic development on middling powers, the role of technology corporations in warfare, and aspects of a plausible future based on these trends. Finally, the paper looks at how U.S. strategic interests may be affected, concluding with suggestions for future research.

"Governments are no longer the only or even the primary targets of sophisticated intelligence collection or cyberattacks: corporations fall within the geopolitical battlespace."

Core Functions of States and Private Entities

The modern state separates the functions of the state from those of private entities. Their governments take on three specific functions: revenue mobilization, adjudicating disputes, and a "monopoly on violence."[4] In short, states are concerned with money, law, and security. Only in the twentieth century have all these functions rested entirely (or been intended to) within the state; before World War II and decolonization, corporations and private entities played a role in them. For example, from the end of the Second National Bank to the creation of the Federal Reserve, private banks helped manage the U.S. monetary system. Private entities participating in the adjudication of disputes include the Saxon frankpledge in medieval England, Pinkerton's protection of railroads, and the American Protective League during World War I.

For much of recorded history, the central government did not have a monopoly on violence. During the European Medieval Period, knights served an important role in warfare, but they were not always sworn to the king. Rather, they would swear fealty to a local lord, who would decide whether they would support the king. During the Renaissance, mercenaries played an essential role in warfare; for example, Italian city-states could not raise sufficient armies and would have to pay sell-swords for their services. During the American Revolution, Britain hired Hessian mercenaries while the would-be United States used privateers.

No corporation in history represents a private entity taking over the core functions of the state better than the East India Company and its rule over South Asia from the mid-1700s to the mid-1800s. The East India Company had its own armies, warships, diplomats, and currencies.[5] Although the East India Company arrived in India in 1612, it did not take on major noneconomic functions until after the Battle of Plassey in 1757. Plunders of war and conquest combined with the monopoly on trade gave the East India Company sufficient funds to hire administrators, revenue collectors, and surveyors.[6] In fact, land taxes on locals would be an important source of revenue for the company when it began to lose its monopoly. The company would continue to fight against competitors and Britain's enemies (especially the French) for the next several decades and was the region's predominant power by 1815.[7]

The East India Company and these other examples show that governments have regularly used, worked with, or allowed private entities to participate in governance, especially security. The increasing participation of multinational technology companies in the core state function of security is a return to that history rather than a new aberration. What has changed, though, is that corporations are the critical private entities that participate in that function and their influence and ubiquity in the modern world have made them essentially geopolitical actors that contribute to the balance of power. Before exploring this trend and its implications, this paper explains the aspects of the core function of security, how cyber technology has altered how governments approach those aspects, and the role corporations (directly or indirectly) have taken in them.

[4] This idea comes from Max Weber's 1919 essay "Politics as a Vocation."

[5] James Morris, *Pax Britannica: The Climax of an Empire* (New York: Harcourt Brace & Company, 1968), 85.

[6] Lawrence James, *The Rise & Fall of the British Empire* (London: Abacus, 1998), 131.

[7] James, *Rise & Fall*, 123. James notes that the "Company owned the most powerful army in India and governed, directly and indirectly, Bengal, much of the upper Ganges basin and extensive areas of eastern and southern India."

Examples of Corporations Taking on the Core Function of Security

This paper looks at how multinational tech corporations are taking on the core state function of security and how that could impact the balance of power in Asia, so it is important to understand the five aspects of that function:

- Use of force in conflict
- Defense of infrastructure and borders
- Intelligence gathering
- Covert operations
- Economic and technological development of power projection

The United States has led the way in using cyber technology for national security purposes, and Asian nations are likely to emulate this as they develop their own cyber capabilities. Journalist Shane Harris documented the "rise of the military-Internet complex" in his book *@War*. He said that while governments traditionally kept nations safe, "government and industry formed an alliance against a common threat" during the inchoate Global War on Terror.[8] Accordingly, U.S. corporations, wittingly or unwittingly, have played a role in the trend of private entities taking on aspects of the core function of security, in cooperation with states and independently. The examples in this section illustrate how states and corporations have increasingly employed cyber technology in national security. These examples provide useful context for the following sections of the paper, which will ask the reader to imagine a future when corporations take on more of these roles. What could this shift look like? How might this shift affect power dynamics in Asia?

Use of Force in Conflict

National security leaders have noted that "the consequences of another major terrorist attack on American soil pale in comparison with the havoc and panic a determined and malicious group of hackers could cause."[9] The George W. Bush presidency from 2001–09 saw the first American uses of force in cyberspace. These would fundamentally alter how the United States engaged in warfare. During the 2007 surge in Iraq, the U.S. military utilized a center of operations at Balad Air Base, where drone pilots worked with National Security Agency (NSA) hackers, Federal Bureau of Investigation (FBI) cyber forensics investigators, and special operations forces to target insurgents.[10] Signals intelligence from electronic communications and further intelligence from hardware investigations (laptops, cell phones, thumb drives, etc.) provided targeting data that were previously inconceivable. NSA hackers were even able to infiltrate al-Qaeda's network of websites and servers, essentially their corporate intranet.[11] This cyber aspect of the operation was critical to the success of the surge.

[8] Shane Harris, *@War: The Rise of the Military-Internet* Complex (Boston: Houghton Mifflin Harcourt, 2014).

[9] Harris, *@War*, xviii.

[10] Harris, *@War*, 17.

[11] Harris, *@War*, 19.

Defense of Infrastructure and Borders

Multiple types of *threat actors*—nation states, terrorists, and criminals—must be countered throughout cyberspace, not just on social media. Tech corporations can play a helpful role in this by targeting the insurgents' online infrastructure, while governments can focus on offensive operations. Microsoft played a key role in combatting Strontium (Microsoft's name for APT28, Fancy Bear)[12] when the company disrupted and transferred control of six internet domains created by the group.[13] According to Microsoft, between 2016–18, they used this approach twelve times to shut down eighty-four fake Strontium websites. In December 2021, Microsoft announced that it had stopped the espionage attempts of Chinese-backed hackers Nickel (APT15, Vixen Panda) by seizing more than forty websites used to gather intelligence on governments, think tanks, and NGOs in twenty-nine countries.[14]

Propaganda and disinformation are quintessential recruiting avenues for terrorists, insurgents, and other adversaries, so combatting it online is now fundamental to national defense.[15] Social media and technology companies are already working to combat the spread of violent content online. Currently, the Global Internet Forum to Counter Terrorism, an organization formed by tech companies like Meta and Microsoft, is working to expand the types of extremist content shared between companies in a key database of hashes[16] used to identify and remove content.[17] As Kent Walker, Google's President for Global Affairs, put the issue, "While governments and civil society groups face a complex challenge in deterring terrorist violence, collaboration across the industry to responsibly address terrorist content online is delivering progress."[18]

Intelligence Gathering

Immediately after 9/11, the U.S. government created intelligence tools to collect and analyze communications from all over the world that went beyond what was previously possible—or accepted. Reading communications is not a new type of intelligence gathering. However, the NSA's Stellarwind program took this to an unprecedented level through its communication and metadata collection.[19] Stellarwind allowed the NSA to gather significantly more information about foreign terrorist organizations and the nature of their communications. Intelligence fundamentally changed because multinational telecommunication companies' global reach allowed the U.S. government to intercept messages sent anywhere. The NSA had the ability to gather and analyze the requisite metadata primarily because of its connections

[12] Strontium (Fancy Bear) is an advanced persistent threat (APT) that is likely connected to Russian military intelligence. An APT is a highly sophisticated threat actor capable of prolonged, clandestine targeting.

[13] Brad Smith, "We Are Taking New Steps against Broadening Threats to Democracy," Microsoft, August 20, 2018, https://blogs.microsoft.com/on-the-issues/2018/08/20/we-are-taking-new-steps-against-broadening-threats-to-democracy/.

[14] Zaini Majeed, "Microsoft Foils China's Espionage on 29 Nations; Seizes 42 Websites Used by Hackers," Republic World, December 7, 2021, https://www.republicworld.com/technology-news/other-tech-news/microsoft-foils-chinas-espionage-on-29-nations-seizes-42-websites-used-by-hackers.html.

[15] Brendan Koerner, "Why ISIS Is Winning the Social Media War," Wired, April 2016, https://www.wired.com/2016/03/isis-winning-social-media-war-heres-beat/; Georgia Wells, "Islamic State's TikTok Posts Include Beheading Videos," *Wall Street Journal*, October 23, 2019, https://www.wsj.com/articles/islamic-states-tiktok-posts-include-beheading-videos-11571855833.

[16] A hash is a number value of a specified length produced from using a hash function on data, such as a file. This allows users to guarantee that the data has not been altered because any changes to the data would create a different hash.

[17] Elizabeth Culliford, "Facebook and Tech Giants to Target Attacker Manifestos, Far-Right Militias in Database," Reuters, July 26, 2021, https://www.reuters.com/technology/exclusive-facebook-tech-giants-target-manifestos-militias-database-2021-07-26/.

[18] Kent Walker, "To Stop Terror Content Online, Tech Companies Need to Work Together," Google, December 20, 2018, https://www.blog.google/outreach-initiatives/public-policy/stop-terror-content-online-tech-companies-need-work-together/.

[19] To understand the complete story of Stellarwind, see Michael Hayden, *Playing to the Edge: American Intelligence in the Age of Terror* (New York: Penguin Press, 2016), 64–91.

to the private sector and backdoors it had placed in a number of companies' products.[20] The Snowden leaks changed the NSA's ability to gather metadata because companies learned about the back doors and closed them. In addition, many companies are working on end-to-end encryption that would make it significantly harder or outright impossible for the NSA to collect the metadata.[21]

Besides the government exploiting corporations for intelligence, private entities can now gather their own. Intelligence gathering and analysis had been only in the purview of governments that had resources to expend on information collection and analysis, but the internet has essentially allowed any enterprising individual or group to create open-source intelligence (OSINT). This could provide a boon to the government because it could leverage hundreds of analysts in the private sector who are already gathering intelligence for their companies. Professor Amy Zegart and former Deputy Director of Central Intelligence Michael Morell have noted, "The combination of new technologies and the rising number, complexity, and velocity of threats means more danger for the United States—and greater demands on its intelligence agencies."[22] One example is Bellingcat, a private organization that uses crowd-sourced OSINT; it proved the true origin of the missile that brought down Flight MH17 over Ukraine.[23] Corporate and private intelligence groups could easily assist a state's national security efforts by providing similar OSINT capabilities to combat terrorism or monitor geopolitical situations.

Covert Operations

Stellarwind and the surge demonstrate how defense capabilities changed because of the role tech companies play in the modern world, but the best example of the reach of tech companies and how they can be exploited is the Stuxnet attack on Iran's nuclear program. Stuxnet was a multiyear, multiagency, multicountry effort to slow down Iran's nuclear program by targeting centrifuges at its Natanz facility. A beautifully written code that included extremely limited targeting and dissemination capabilities to prevent mass infections, Stuxnet was successful because the coders burned four zero-day vulnerabilities to infect the computers and industrial control systems in Natanz.[24] The zero days that Stuxnet targeted were in Microsoft Windows, which had a number of vulnerabilities that allowed it to be successful.[25] Microsoft's reach into an authoritarian country that was running an illegal nuclear program allowed the U.S. government to target and exploit vulnerabilities within that company's software to achieve its aims.

[20] A backdoor is a deliberate vulnerability that gives third parties special access to systems by circumventing the normal security protocols. See "Spy Agency Ducks Questions about 'Back Doors' in Tech Products," Reuters, October 28, 2020, https://www.nbcnews.com/tech/security/spy-agency-ducks-questions-back-doors-tech-products-rcna167.

[21] David E. Sanger and Nicole Perlroth, "Encrypted Messaging Apps Face New Scrutiny over Possible Role in Paris Attacks," *New York Times,* November 16, 2015, https://www.nytimes.com/2015/11/17/world/europe/encrypted-messaging-apps-face-new-scrutiny-over-possible-role-in-paris-attacks.html.

[22] Amy Zegart and Michael Morrell, "Spies, Lies, and Algorithms," *Foreign Affairs,* May/June 2019, https://www.foreignaffairs.com/articles/2019-04-16/spies-lies-and-algorithms.

[23] Charlie Savage, "The Rise of Private Spies," *New Republic,* May 10, 2021, https://newrepublic.com/article/161913/we-are-bellingcat-spooked-private-investigators.

[24] A zero-day vulnerability is a vulnerability that has not been discovered or patched, so threat actors can exploit it.; Kim Zetter, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon* (New York: Broadway Books, 2014), 90.

[25] Zetter, 90. These vulnerabilities included included MS08-067 from the Conficker attack, a .lnk flaw (Windows shortcut), and even one in the print spooler service that would let the virus spread between machines that shared a printer.

Development of Power Projection

Tech companies are already working with the Department of Defense,[26] the intelligence community,[27] and law enforcement in a number of ways, and former Defense Secretary Ash Carter has specifically noted the benefit of government working with the technology sector.[28] Technology companies are directly contributing to power projection—states' ability to deploy force outside their borders—through contracts with the government, such as providing cloud services or developing augmented reality/virtual reality (AR/VR) technologies to be used by the military.

Technology has profoundly altered the ability of states and nonstate actors to harm others and achieve their goals. No other industry or sector touches practically every aspect of national security. Technology companies are used either directly or indirectly to support the defense of infrastructure and covert actions, as in Microsoft's targeting of Russian threat actors to prevent their penetration of important systems. Technology companies have contributed to significant intelligence gathering with data and OSINT, were critical during the Global War on Terror, and are essential components of power projection. Whether it is terrorists needing to host their websites, adversaries communicating about possible attacks, or Iranian nuclear scientists using Windows on their computers, everyone uses technology now. This is why governments, militaries, terrorists, hackers, and others can harm almost anyone anywhere in the world. The next sections will discuss reconfigurations in the Asian balance of power that could result from the increasing role of multinational tech corporations and how governments interact with, for, or against them.

[26] Jackson Barnett, "Microsoft CEO Stresses Importance of Work with the Military," Fedscoop, August 19, 2020, https://www.fedscoop.com/microsoft-dod-partnerships-military-jedi/.

[27] April Glaser, "Thousands of Contracts Highlight Quiet Ties between Big Tech and U.S. Military," NBC News, July 8, 2020, https://www.nbcnews.com/tech/tech-news/thousands-contracts-highlight-quiet-ties-between-big-tech-u-s-n1233171.

[28] Ash Carter, "Why Big Tech and the Government Need to Work Together," Wired, September 14, 2018, https://www.wired.com/story/why-big-tech-and-the-government-need-to-work-together/.

Trends and the Future: China and Tech Corporations

China is undergoing a number of economic and political changes. These probably will shift the role of corporations in security because of regulations their government is imposing on markets. These regulations could lead corporations to become more aggressive in their pursuit of innovation because of a lack of capital and lead to a larger role for Chinese companies in intelligence gathering and covert operations, especially when the targets of those actions are other technology companies. Intelligence gathering and covert operations could give the Chinese government and corporations a comparative advantage through the theft of intellectual property, which could affect middling powers in the region.[29]

President Xi Jinping's leadership has focused on trying to distinguish the Chinese economic system from a Western capitalism that is laissez-faire and less directed by the state.[30] As the government takes more control over corporate behavior, this will impact how China's economy develops and the role tech companies play in geopolitics. China's economic liberalization, which started with Deng Xiaoping, led to millions being lifted out of poverty and created significant wealth for the country. Many theorists in the West thought economic liberty would be a precursor to political liberty. However, Xi's recent policy changes are undoing that liberalization. Xi is acting not only out of a desire for more political power but also ideologically: He wants to turn China into a "modern socialist power" with "common prosperity."[31] Several regulatory actions have been imposed by the Chinese government, such as breaking up the monopolistic dominance of Alibaba,[32] Tencent Holdings,[33] and Didi Global[34] in their respective markets. These regulations have also increased state supervision of foreign capital, which may reduce the interconnectedness of the global economy and increase the possibility of conflict.[35] As an example of the economic impact of such actions, Xi's regulatory policies eliminated more than $1 trillion in stock market value[36] and threatens more than

> **"Intelligence gathering and covert operations could give the Chinese government and corporations a comparative advantage."**

[29] A middle power in international relations refers to a state with moderate influence but not enough resources or strength to be a great power.

[30] Lingling Wei, "Xi Jinping Aims to Rein in Chinese Capitalism, Hew to Mao's Socialist Vision," *Wall Street Journal*, September 20, 2021, https://www.wsj.com/articles/xi-jinping-aims-to-rein-in-chinese-capitalism-hew-to-maos-socialist-vision-11632150725?mod=itp_wsj&mod=djemITP_h.

[31] Ibid.

[32] Keith Zhai and Lingling Wei, "China Lays Plans to Tame Tech Giant Alibaba," *Wall Street Journal*, March 11, 2021, https://www.wsj.com/articles/china-regulators-plan-to-tame-tech-giant-alibaba-jack-ma-11615475344.

[33] Lingling Wei and Stephanie Yang, "China Warns Large Tech Firms as Industry Faces Rising Oversight," *Wall Street Journal*, April 29, 2021, https://www.wsj.com/articles/chinese-financial-regulators-summon-big-tech-firms-11619698257.

[34] Lingling Wei, "Chinese Regulators Suggested Didi Delay its U.S. IPO," *Wall Street Journal*, July 5, 2021, https://www.wsj.com/articles/chinese-regulators-suggested-didi-delay-its-u-s-ipo-11625510600?mod=mktw&mod=.

[35] Erik Gartzke, "The Capitalist Peace," *American Journal of Political Science* 51, no. 1 (January 2007): 166-91.

[36] Jing Yang, Keith Zhai, and Quentin Webb, "China's Corporate Crackdown Is Just Getting Started: Signs Point to More Tumult Ahead," *Wall Street Journal*, August 5, 2021, https://www.wsj.com/articles/china-corporate-crackdown-tech-markets-investors-11628182971?mod=article_inline.

$3 trillion of other stocks.[37] President Xi probably pursued this regulatory course because the power of technology companies expanded and "the growing influence of these private firms was having the effect of reducing the power of the state and the CCP."[38]

An overly regulated market probably would reduce foreign direct investment, but corporations would still need capital to fund research and development. To support such industries, China would need to find other avenues that lead to innovation. One possible path is intellectual property theft. While trying to control its own corporations, the Chinese government has strongly supported attacks on and theft from many other corporations throughout the world. U.S. Department of Justice officials have especially noted the threat from China on this issue. In February 2020, the FBI was investigating 1,000 incidents of Chinese theft of U.S. technology.[39] Although most of these cases included theft of intellectual property, there is an increasing risk that state actors or corporations may steal prototypes and other high-value assets from tech companies in order to advance their research on controversial or complicated subjects, such as virtual reality and artificial intelligence.

An infamous case of intellectual property theft on behalf of a state is that of Stephen Su, a Chinese businessman who stole secrets from Boeing, Lockheed, and other U.S. companies for years before he was discovered.[40] Su's small company, Lode-Tech, manufactured aircraft cable harnesses, but from 2009 to 2014 he established a network of business contacts in major firms. By befriending important industry insiders, Su was able to gain information about Lockheed Martin's F-35 and F-22 and Boeing's C-17. Su would identify the requisite information and personnel, and his colleagues would hack the company and steal the information.

China's attitude toward domestic and international technology companies is hostile, which leads to limiting their organic development while promoting theft of intellectual property and data from foreign corporations. This combination may increase conflict because companies could be expected to deliver innovative solutions and expand economically, but more and more espionage may be required to achieve those goals. The rest of this section explores a plausible future based on these trends in China.

Plausible Future: Challenges for China and Reconfiguration

Over the next two decades, China may decline relative to other regional powers, which would provide opportunities for middling powers to gain comparative economic and technological advantages. Xi's new approach to corporations may lead to significantly lower economic growth than in the 1990s and 2000s, which may cause China's economic strength to decline compared to its neighbors. Those problems are likely to be exacerbated by other societal factors, such as a sex imbalance that resulted from the One Child Policy, slower population growth, and overextended property development. However, the crux of the problem may be a burdensome regulatory environment that makes innovation incredibly difficult. Not only would that hamper China's development, but it would also lead to less foreign investment and cooperation with foreign companies, especially American ones. A lack of capital inflow over fears that the Chinese government may take control of companies or projects would further reduce economic development.

China depends on economic growth to meet important areas of domestic demand and maintain political support,

[37] Yen Nee Lee, "Goldman Sachs Says $3.2 Trillion Worth of Chinese Stocks at Risk of Further Regulatory Crackdown," CNBC, September 16, 2021, https://www.cnbc.com/2021/09/16/china-stocks-worth-trillions-at-risk-of-more-regulations-goldman-sachs.html.

[38] Daniel Rosen, "Xi Is Running Out of Time," *Foreign Affairs*, November 5, 2021, https://www.foreignaffairs.com/articles/china/2021-11-05/xi-running-out-time?utm_campaign.

[39] Catalin Cimpanu, "FBI Is Investigating More than 1,000 Cases of Chinese Theft of US Technology," ZDNet, February 8, 2020, https://www.zdnet.com/article/fbi-is-investigating-more-than-1000-cases-of-chinese-theft-of-us-technology/.

[40] Jim Sciutto, *The Shadow War: Inside Russia's and China's Secret Operations to Defeat America* (New York: Harper, 2019).

so it may respond to these negative developments by significantly increasing its theft of intellectual property from U.S., European, and other Asian technology companies. The Chinese Communist Party (CCP) may use its 5-year plans to help coordinate the actions of threat actors by letting patriotic hackers and those who work with state security services know which industries to target. Theft of intellectual property would reinforce other countries' refusal to work with China and Chinese companies, leading to even more aggressive attacks by China against tech companies in the West and Asia. Other nations and technology companies would then respond more aggressively themselves, increasing the likelihood of conflict between China, corporations, and other countries.

China's regulatory controls and lack of development could lead to the rise of middling powers that are able to develop technology companies and gain greater access to foreign capital. Increased regulatory controls in China would mean less profit for multinational tech companies, so those companies would look elsewhere to invest in innovation and new technologies. Many countries in Asia are limited by natural resources and smaller industrial bases, but technology companies can grow without those factors. Even creating simple apps for commerce or ride sharing can bring in hundreds of millions to billions of dollars in investment and revenue. U.S. corporations are an excellent example of how small technology companies that focus on a specific area can flourish in whole industries and lead to creative destruction. For example, Amazon started as an online bookstore; morphed into a full ecommerce site; and now has cloud contracts with the government, owns a grocery store chain, and even sells its own products. Smaller countries are likely to see that kind of growth, which would give them the economic clout to challenge China over geopolitical issues. China's failures to handle technological development through innovation rather than theft, combined with its overly burdensome regulatory approach, may indirectly lead to the rise of middling powers in Asia based on their own tech companies. These middling powers may be more willing to challenge China to prevent its regional hegemony.

Trends and the Future: National Development and Tech Companies

Security threats to technology companies, and therefore to the security of countries, is altering how governments in Asia regulate technology and changing their domestic industries. In particular, the balkanization of technology through regulations and trade barriers could require corporations to take on a greater role in the development of power projection.[41] Historically, states have determined the kind of weaponry they needed or thought they would need, and then they funded research or contracts to have those weapons developed. Now, however, technology companies, especially unicorns,[42] are a critical locus of power. They allow countries to rely on domestic companies for the other four aspects of the security state function (use of force, defense of infrastructure, intelligence gathering, and covert operations). This could lead to the rise of middling powers in Asia as security requirements and balkanization encourage them to build up their domestic industries.

The growth of middle powers in Asia will probably be accompanied by increased scrutiny from countries with advanced economies, especially China, and the rise of technonationalism.[43] Japanese Prime Minister Fumio Kishida has called for a "new capitalism" that would abandon the neoliberalism of the past decades and add a kind of economic nationalism.[44] This would bolster Japan's economic position and serve security purposes. In February 2022, Japan considered imposing restrictions on purchasing foreign software in security-sensitive sectors in order to counter cyberattacks.[45] Kishida wants to better defend Japan against China's economic espionage and attacks, and he wants to prevent the theft of sensitive technology while creating a more resilient supply chain. The proposed regulations would give the government the power to review purchases if the software or equipment could increase the likelihood of a cyberattack.

Because of security concerns, democracies and autocracies are even balkanizing the internet, which is the splintering of the internet's infrastructure or content. Splintering can occur through regulations or technologies, and it can be done through blocking websites or IP ranges, countries having their own intranet, or other mechanisms. This is leading to a "world fractured between competing national or ideological blocs, each relying on its own trusted hardware and software suppliers to defend against malign interference."[46] Authoritarian governments advocate

[41] The World Wide Web is open by default, so if governments want to limit access, they have to impose barriers through regulations, technology, and other means. This is called the balkanization of the internet or sometimes the splinternet because the internet would be splintered or broken up (balkanized).

[42] A unicorn is a tech company with a valuation of at least $1 billion. For example, Indonesia already has five unicorns, including the ridesharing Gojek, online marketplace Tokopedia, and digital payment service OVO. See Tech Collective, "We Take a Closer Look at the Indonesian Unicorn Startups," Tech Collective, February 21, 2021, https://techcollectivesea.com/2021/02/22/we-take-a-closer-look-at-the-indonesian-unicorn-startups/.

[43] Technonationalism is a mercantilist approach that connects technology and innovation to a country's security and prosperity.

[44] Masato Shimizu, "Kishida's 'New Capitalism' Raises Economic Reform Setback Fears," Nikkei Asia, October 5, 2021, https://asia.nikkei.com/Politics/Inside-Japanese-politics/Kishida-s-new-capitalism-raises-economic-reform-setback-fears.

[45] "Japan Eyes Tighter Curbs to Counter Cyber Attacks," *Straits Times*, February 3, 2022, https://www.straitstimes.com/tech/tech-news/japan-eyes-tighter-curbs-to-counter-cyber-attacks.

[46] Graham Webster and Justin Sherman, "The Fall and Rise of Techno-Globalism," *Foreign Affairs*, October 28, 2021, https://www.foreignaffairs.com/articles/world/2021-10-28/fall-and-rise-techno-globalism.

“Security threats to technology companies, and therefore to the security of countries, is altering how governments in Asia regulate technology and changing their domestic industries.”

cyber sovereignty so they can regulate the information their residents or citizens can consume. China has even required Amazon to remove unflattering reviews of Xi’s book. Democracies have also sought to regulate software out of geopolitical concerns. For example, Secretary of State Mike Pompeo’s Clean Network initiative wanted to expel untrusted Chinese apps, and Indian Prime Minister Narendra Modi has continued a 2020 ban on certain Chinese software apps.[47]

Balkanization of the internet would probably lead to more confrontation and less restraint between countries because less interdependence would mean lower opportunity costs and less risk of blowback when cyberattacks occur. This would significantly increase the likelihood of attacks by advanced persistent threats (APTs) or state actors on critical infrastructure that could cause physical harm and conflict. Even Lithuania has participated in balkanization efforts over security concerns, further disconnecting the technologies used by each region. In September 2021, the Lithuanian Defense Ministry recommended consumers not purchase Chinese mobile phones and advised those who had purchased such phones to get rid of them.[48] The Defense Ministry was concerned over “built-in censorship capabilities,” as the Xiaomi Corporation had software that could detect and censor terms the CCP opposes, including “Free Tibet,” “Long live Taiwan independence,” and “democracy movement.” The closing of countries to specific foreign corporations is not a new economic concept. Mercantilism and certain types of capitalism used trade barriers to help domestic industries. However, that is not quite the motivation for this new round of economic barriers. Strategic economic competition requires the security of capital and infrastructure, but security threats, mostly from China, have made more Asian countries leery. The rest of this section describes a plausible future.

Plausible Future: Balkanization and Reconfiguration

The rise of middling economic powers through the contributions of their technology companies might occur in context with increased trade barriers that result from economic nationalism, security concerns, and the balkanization of the internet. Countries like South Korea, India, Vietnam, and the Philippines are likely to follow Japan and limit the purchase of foreign devices and software that could harm critical infrastructure and sectors. This could force countries to be more selective in their trading partners and create trusted blocs for economic development. Historically, great power competition has taken similar paths. Despite the British Empire’s alleged defense of free trade during the height of its power, what it really did was create a free trade bloc within the empire while pushing out other possible trading partners, such as France. Free trade was only selectively used—domestic industries were preferred. Over the next few decades, a similar approach might occur in Asia as nationalist interests override any alleged devotion to free trade.

Thus, countries would have to put a lot more resources into their domestic industries to ensure they can remain competitive. Subsidies or other trade barriers are regularly used to help companies that are connected to a country’s strategic interests, but these would have to expand even further. They would cover not only manufacturing and software development but also critical inputs into these industries, such as rare earth metals and neon gas for lasers.

[47] Ibid.

[48] Andrius Sytas, “Lithuania Says Throw Away Chinese Phones due to Censorship Concerns,” Reuters, September 21, 2021, https://www.reuters.com/business/media-telecom/lithuania-says-throw-away-chinese-phones-due-censorship-concerns-2021-09-21/.

There would be increased domestic development at every part of the supply chain in tech development, such as manufacturing computer chips. The private sector would be unlikely to be able to handle all this on its own, which means governments in Asia may need to greatly expand their investment budgets. National priorities would have to shift overwhelmingly to the technology sector for middling powers to achieve a higher economic status.

The most negative impact of this would be a significant decline in economic interdependence, which has been a mitigating factor for conflict. Although economic integration does not completely prevent wars, it does make states more judicious in choosing when, where, and how to use force for fear of disrupting their own economic activity. Without those economic connections, there could be a higher probability of conflict, especially conflict in the cyber realm or fifth domain.

Trends and the Future: Cyber Conflict and Corporations

The core function of security has its greatest impact during war. This section looks at how corporations are taking on an important role in the use of force, including as targets, mercenaries, and attackers. During the 2020 border conflict between China and India, businesses were targeted as a matter of course, and they had to provide defense for their own infrastructure. American companies like Microsoft have already taken on a significant role in infrastructure security. Their direct targeting of state threat actors is akin to the use of force in conflict and covert operations. Cyber arms dealers, such as Exodus and NSO Group, play a role in the development of power projection. Major tech companies are also providing a significant amount of intelligence on threat actors and state activity to the public and government. The role of corporations in warfare and conflict shows how tech companies have already been involved in the use of force, particularly in direct cyberattacks, as cyber arms dealers, and in infrastructure security.

> **"The role of corporations in warfare and conflict shows how tech companies have already been involved in the use of force, particularly in direct cyberattacks, as cyber arms dealers, and in infrastructure security."**

Corporate Role in the Use of Force

Direct cyberattacks. Warfare has often targeted economic centers of gravity in an attempt to disrupt the lives of enemies. Technology companies may be targeted in smaller, purely punitive attacks more often in coming decades. Corporations, especially tech corporations, may be the target of more attacks as states seek to advance their interests. In summer 2020, China engaged in major offensive cyber operations against Australia and India. In mid-June, Indian and Chinese military forces clashed in Ladakh, a disputed Himalayan border area.[49] The incident occurred after increased tensions between India and China, and it led to the death of a few dozen Indian soldiers (it is not known how many Chinese soldiers died). As part of the conflict between the two countries, China engaged in cyberattacks against India's information technology infrastructure and banking sector. According to some reports, China attempted more than 40,000 cyberattacks, such as denial of service attacks, hijacking of internet protocols, and phishing; these directly impacted corporations in India.[50] Around the same time, Australia was attacked by a sophisticated state actor, probably China.[51] Prime Minister Scott Morrison stated the cyberattacks were widespread and covered "all levels of government" along with essential services and businesses. According to Morrison, the targets included "government, industry, political organisations, education, health, essential service providers and operators of other critical infrastruc-

[49] "India-China Clash: 20 Indian Troops Killed in Ladakh Fighting," BBC, June 16, 2020, https://www.bbc.com/news/world-asia-53061476.

[50] "Chinese Hackers Attempted 40,000 Cyber Attacks on Indian Web, Banking Sector in 5 Days," *India Today*, June 24, 2020, https://www.indiatoday.in/india/story/chinese-hackers-attempted-40-000-cyber-attacks-on-india-1692088-2020-06-24.

[51] Australian Associated Press, "Mike Pompeo Blasts China's 'Coercion' of Australia as Cyber-Attack Likened to Parliament House Hack," *Guardian*, June 19, 2020, https://www.theguardian.com/world/2020/jun/20/mike-pompeo-blasts-chinas-coercion-of-australia-as-cyber-attack-likened-to-parliament-house-hack; Kieran Corcoran, "Australia Is All but Accusing China of a Months-Long Cyberattack on its Government Systems and Major Companies," Business Insider, June 19, 2020, https://www.businessinsider.com/australia-all-but-accuses-china-cyberattack-government-companies-2020-6.

ture."[52] In these incidents, China targeted businesses to punish India and Australia over border and trade issues. This made the companies part of the geopolitical conflict even though they did not directly participate in it.

Cyber arms dealers. One area in which corporations play a central role in cybersecurity and cyberwar is by acting as mercenaries and suppliers of arms that can help with espionage or offensive capabilities, such as selling software with zero-day vulnerabilities that can be used for espionage and offensive purposes. Governments store zero-day vulnerabilities for cyberattacks in hopes that companies do not become aware of the vulnerabilities and patch them before they can be used. The companies that find, buy, and sell zero days get to choose their customers based on their values. For example, Exodus Intelligence, a Texas-based company, investigated whether India used such a vulnerability to spy on Pakistan and China by gaining deep access to Microsoft's operating system.[53] In response to this espionage campaign, Exodus stopped selling their zero-day research to India. While companies like Exodus have attempted to have an ethical customer base, other cyber mercenaries have chosen to align with whoever will pay. One of the most nefarious of such companies is the NSO Group. The NSO Group, which also goes by Q Cyber Technologies, was founded in Israel in 2010 by Omri Lavie with funding from veterans of the Israeli Defense Force's 8200 intelligence unit. NSO has become one of the preeminent private spying companies in the world, with a focus on the exploitation of mobile phones.

In 2016, the NSO Group found three zero days in an unpatched iOS that allowed hackers to silently jailbreak the phone with only the click of a link by the user.[54] This allowed the company to install Pegasus, a malware that one journalist described as the "most invasive mobile spy kit."[55] Pegasus stole all communications and locations of the targeted iPhones, including iMessage, Gmail, Viber, Facebook, WhatsApp, Telegram, and Skype communications, along with other data like Wi-Fi passwords. Interestingly, NSO's founders helped found Kaymera, a company that focuses on protecting phones from the kind of hackers who would use Pegasus.[56] Pegasus spyware evolved, and NSO developed a method to compromise phones without requiring a malicious link to be clicked.[57] In July and August 2020, thirty-six personal phones of journalists were compromised by the KISMET exploit chain. KISMET was a zero-day vulnerability of at least iOS 13.5.1 that allowed the hacking of Apple's then-latest iPhone 11. It does not appear that KISMET works against iOS 14. The NSO Group also found a way to exploit WhatsApp and inject malware with a missed phone call. WhatsApp has encrypted messaging by default, but in 2019 NSO exploited a bug within VoIP that was triggered without the user picking up the call.[58] According to Facebook, the WhatsApp vulnerability stemmed from an extremely common type of bug known as a buffer overflow.[59]

[52] "Australia Cyber Attacks: PM Morrison Warns of 'Sophisticated' State Hack," BBC, June 19, 2020, https://www.bbc.com/news/world-australia-46096768.

[53] Thomas Brewster, "An American Company Fears its Windows Hacks Helped India Spy on China and Pakistan," Forbes, September 17, 2021, https://www.forbes.com/sites/thomasbrewster/2021/09/17/exodus-american-tech-helped-india-spy-on-china/.

[54] Jailbreak is removing software restrictions installed by the manufacturer so a user can have unrestricted access to the file system. Unpatched means that a company has not released an update to fix a vulnerability.

[55] Thomas Brewster, "Everything We Know about NSO Group: The Professional Spies Who Hacked iPhones with a Single Text," Forbes, August 25, 2016, https://www.forbes.com/sites/thomasbrewster/2016/08/25/everything-we-know-about-nso-group-the-professional-spies-who-hacked-iphones-with-a-single-text/.

[56] Gabriella Coppola, "Israeli Entrepreneurs Play Both Sides of the Cyber Wars," Bloomberg, September 29, 2014, http://www.bloomberg.com/news/2014-09-29/israeli-entrepreneurs-play-both-sides-of-the-cyber-wars.html.

[57] Bill Marczak, John Scott-Railton, Noura Al-Jizawi, Siena Anstis, and Ron Deibert, "The Great iPwn," Citizen Lab, December 20, 2020, https://citizenlab.ca/2020/12/the-great-ipwn-journalists-hacked-with-suspected-nso-group-imessage-zero-click-exploit/.

[58] Lily Hay Newman, "How Hackers Broke WhatsApp with Just a Phone Call," Wired, May 14, 2019, https://www.wired.com/story/whatsapp-hack-phone-call-voip-buffer-overflow/.

[59] "CVE-2019-3568," Facebook, August 13, 2019, https://www.facebook.com/security/advisories/cve-2019-3568.

NSO Group has publicly stated that the company "sells only to authorized governmental agencies, and fully complies with strict export control laws and regulations. Moreover, the company does NOT operate any of its systems; it is strictly a technology company."[60] However, the NSO Group's clients are allegedly not only "authorized government entities;" the company has been accused of working with autocratic or even totalitarian regimes under the guise of combatting transnational crime and terrorism.[61] NSO Group represents the kind of cyber mercenaries that may become more common, selling zero days, software, and exploits to any government willing to pay for them. These weapons could be used in offensive operations against corporations and governments. Such cyber mercenaries would very probably be used by governments in Asia during conflict, especially by middle powers without well-established offensive cyber agencies. It would be easier for them to purchase vulnerabilities and exploits than build their own.

Infrastructure security. The final area of cyber conflict that technology companies have a role in is working to support national defense with infrastructure security. Examples include the SolarWinds attack on U.S. supply chains,[62] a ransomware attack on the U.S. energy sector (Colonial Pipeline),[63] and even a hack of the Microsoft Exchange server.[64] As one *New York Times* article put it, "Ransomware attacks are striking every eight minutes, crippling hospitals and American mainstays like gas, meat, television, police departments, NBA basketball and minor league baseball teams, even ferries to Martha's Vineyard."[65] Corporations are not just being attacked directly. According to Paul Myerson in *Industry Weekly*, 80% of cyber breaches occur in the supply chain.[66] Crafting a stronger response than previous administrations, the Biden administration moved on several fronts to try and better protect the U.S.'s critical infrastructure. President Biden issued a directive for federal agencies to establish cybersecurity goals for companies considered critical infrastructure because of the onslaught of ransomware attacks in 2020–21, such as the Colonial Pipeline and SolarWinds attacks.[67] In response to the Colonial Pipeline ransomware attack, Anne Neuberger, the National Security Council's top cyber official, issued an open letter to the private sector on ransomware prevention that recommended steps such as segmenting networks and having reliable recovery plans.[68] In addition, the Department of Justice is giving

> **"Tech companies already take an active role in the defense of critical infrastructure."**

[60] Brewster, "Everything We Know."

[61] "Read the Intelligence Report Implicating Saudi Arabian Crown Prince Mohammed bin Salman in the Killing of Journalist Jamal Khashoggi," *Washington Post*, February 26, 2021, https://www.washingtonpost.com/context/intelligence-report-jamal-khashoggi-saudi-arabia/501b6e72-f6c5-42e5-bb3a-1e2eeedfaf30/?itid=lk_interstitial_manual_10; Matt Burgess, "If Saudi Arabia Did Hack Jeff Bezos, This Is Probably How It Went Down," *Wired*, January 23, 2020, https://www.wired.co.uk/article/jeff-bezos-phone-hack-mbs-saudi-arabia.

[62] Liam Tung, "Microsoft: We've Found Three More Pieces of Malware Used by the SolarWinds Attackers," ZDNet, March 5, 2021, https://www.zdnet.com/article/microsoft-weve-found-three-more-pieces-of-malware-used-by-the-solarwinds-attackers/.

[63] David Sanger and Nicole Perlroth, "Pipeline Attack Yields Urgent Lessons about U.S. Cybersecurity," *New York Times*, June 8, 2021, https://www.nytimes.com/2021/05/14/us/politics/pipeline-hack.html.

[64] Charlie Osborne, "Everything You Need to Know about the Microsoft Exchange Server Hack," ZDNet, April 19, 2021, https://www.zdnet.com/article/everything-you-need-to-know-about-microsoft-exchange-server-hack/.

[65] Nicole Perlroth, "Are We Waiting for Everyone to Get Hacked?," *New York Times*, June 7, 2021, https://www.nytimes.com/2021/06/05/business/leon-panetta-cyber-attacks.html.

[66] Paul Myerson, "Can't Turn Back Time: Cybersecurity Must Be Dealt With," Industry Week, January 3, 2017, https://www.industryweek.com/supply-chain/article/22006116/cant-turn-back-time-cybersecurity-must-be-dealt-with.

[67] Dustin Volz, "Biden Directs Agencies to Develop Cybersecurity Standards for Critical Infrastructure," *Wall Street Journal*, July 28, 2021, https://www.wsj.com/articles/biden-directs-agencies-to-develop-cybersecurity-standards-for-critical-infrastructure-11627477200.

[68] Sarah Coble, "White House Issues Open Letter on Ransomware," *Infosecurity Magazine*, June 3, 2021, https://www.infosecurity-magazine.com/news/white-house-issues-open-letter-on/.

ransomware attacks the same priority as terrorism.[69]

Tech companies already take an active role in the defense of critical infrastructure, such as Microsoft investigating the SolarWinds hack[70] and protecting elections[71] or Rafael Advanced Defense Systems joining twelve leading Israeli cyber companies to protect critical assets.[72] Microsoft's president, Brad Smith, articulated this principle by saying the technology sector needs to "commit to more effective and collaborative leadership by the government and the tech sector in the United States to spearhead a strong and coordinated global cybersecurity response."[73] The government simply does not have the resources to protect every critical industry in the United States, so it must work with tech and cybersecurity companies to enlist their help in protecting infrastructure. This will be a critical defensive action during any conflict, and corporations in Asia will likely need to take on similar roles.

Example: 2022 Russian Invasion of Ukraine

On February 24, 2022, Russia further invaded Ukraine, claiming it was liberating the country from fascists and protecting Russia from NATO expansion. This conflict in Europe has demonstrated several ways in which technology firms might play a critical role in global conflict in the future. The use of corporations to support state activity will probably be emulated in the next war in Asia, making it a useful example to assess. Whether it is social media companies controlling information or tech companies targeting state-sponsored APTs, multinational technology companies are likely to participate directly or indirectly in the next war in Asia.

Early in the war, the Ukrainian government successfully brought many technology companies to its side, along with other nonstate cyber actors. Although there were fewer cyberattacks than security professionals were expecting, tech companies were vital for Ukraine's objectives. For example, Ukraine collected and posted a cache of uncensored satellite images from Google Maps showing Russian military bases and sites.[74] Google was targeted by Russia because the company decided to ban any ad that would "exploit, dismiss or condone" the invasion.[75] The conflict also took place over social media companies. Facebook placed restrictions on state-owned media from Russia, while Twitter placed timeline restrictions on government accounts. Because Facebook (Meta) and Twitter would not comply with Russian demands, the Russian government banned the companies, even calling Facebook an "extremist organization."[76] Social media platforms were not the only ones that tried to contain Russian propaganda and information operations: YouTube blocked access to Russian state-owned media like Russia Today and Sputnik.[77]

[69] Christopher Bing, "U.S. to Give Ransomware Hacks Similar Priority as Terrorism," Reuters, June 3, 2021, https://www.reuters.com/technology/exclusive-us-give-ransomware-hacks-similar-priority-terrorism-official-says-2021-06-03/.

[70] MSRC Team, "Microsoft Internal Solorigate Investigation Update," Microsoft, December 31, 2020, https://msrc-blog.microsoft.com/2020/12/31/microsoft-internal-solorigate-investigation-update/.

[71] Tom Burt, "Innovative New Uses of ElectionGuard," Microsoft, December 4, 2020, https://blogs.microsoft.com/on-the-issues/2020/12/04/electionguard-2020-elections-security-pilot/.

[72] Anna Ahronheim, "Rafael Sets up Cyber Consortium to Defend Critical Infrastructure," *Jerusalem Post*, June 1, 2021, https://www.jpost.com/israel-news/rafael-sets-up-cyber-consortium-to-defend-critical-infrastructure-669769.

[73] Brad Smith, "A Moment of Reckoning: The Need for a Strong and Global Cybersecurity Response," Microsoft, December 17, 2020, https://blogs.microsoft.com/on-the-issues/2020/12/17/cyberattacks-cybersecurity-solarwinds-fireeye/.

[74] Amit Chaturvedi, "Ukraine Says Satellite Photos of Russian Bases Unblurred, Google Denies," NDTV, April 19, 2022, https://www.ndtv.com/world-news/ukraine-says-satellite-photos-of-russian-bases-unblurred-google-denies-2901086.

[75] Alex Hern, "Russia Blocks Google News after Ad Ban on Content Condoning Ukraine Invasion," *Guardian*, March 24, 2022, https://www.theguardian.com/world/2022/mar/24/russia-blocks-google-news-after-it-bans-ads-on-proukraine-invasion-content.

[76] Dan Milmo, "Russia Blocks Access to Facebook and Twitter," *Guardian*, March 4, 2022, https://www.theguardian.com/world/2022/mar/04/russia-completely-blocks-access-to-facebook-and-twitter.

[77] Dave Paresh, "YouTube Blocks Russian State-Funded Media Channels Globally," Reuters, March 11, 2022, https://www.reuters.com/business/media-telecom/youtube-blocks-russian-state-funded-media-channels-globally-2022-03-11/.

Technology companies played a role in mitigating information operations, limiting the spread of propaganda, and assisting the Ukrainian government with their resources, but some also went after Russian threat actors.[78] Microsoft took strong steps against GRU-connected Strontium (APT28, Fancy Bear) in response to the group targeting Ukraine. The company was able to disrupt some of Strontium's attacks by taking control of seven internet domains and redirecting the domains to a sinkhole. Those domains had been used to target government institutions and think tanks in the U.S. and EU along with Ukrainian media organizations. According to Microsoft:

> Before the Russian invasion, our teams began working around the clock to help organizations in Ukraine, including government agencies, defend against an onslaught of cyberwarfare that has escalated since the invasion began and has continued relentlessly… We continue to work closely with government and organizations of all kinds in Ukraine to help them defend against this onslaught.[79]

Microsoft openly acknowledged that it was helping Ukraine in a geopolitical situation, not only by defending its government but also by targeting the Russian threat actors causing the problems. These companies were not coerced by the U.S. government into helping. They did so based on their own geopolitical views and interests, and they have played an important if small role in the war. This conflict is essentially the first case of what is to come in the reconfiguration of global politics. Ukraine brought in every part of the tech and cyber world to defend its territorial integrity and sovereignty.

Plausible Future: Cyber Conflict and Reconfiguration

Balkanization of the internet and decoupling of economies could increase the likelihood of a cyber conflict that could lead to a full-fledged war that might dramatically reshape the balance of power in Asia. Here, corporations may play a critical role, one traditionally reserved for state security services and the military. Technology companies in each country may increasingly play a vital role in defending critical infrastructure and themselves from hostile state attacks. The extent of cooperation between governments and corporations would determine a country's relative power. Much like Microsoft targeting threat actors in the United States and participating in investigations of cyberattacks, technology corporations in middling powers would have to engage in similar actions. The cyber capabilities of the private sector would determine the defense capabilities of the country.

Although corporations would be essential for defending the critical and economic infrastructure of countries, they would also increasingly be targets themselves whenever geopolitical crises unfold, such as when China targeted Indian and Australian businesses over territorial and political disputes, respectively. Whenever there is geopolitical tension, technology companies would be targeted by state actors or patriotic hackers to try and coerce the targets, signal displeasure, or punish them. In future decades, conflict would no longer be cyber or physical or political or economic. Conflict, especially lower level conflict, could involve all factors, particularly when technology companies are targeted in operations.

Power projection by states will also be critical to the balance in Asia. Here again, technology companies might play a role both as participants in operations and as mercenaries. Governments may have significant resources, but they cannot monitor and neutralize threats in all locations. Corporations in the United States are likely to set the example for how corporations act in other parts of the world. One plausible scenario for this development would be legalized *hack backs*, where governments give corporations permission to attack targets in foreign countries that have attacked the company. Mercenary activity would be closely related to this issue as well. More and more com-

[78] Tom Burt, "Disrupting Cyberattacks Targeting Ukraine," Microsoft, April 7, 2022, https://blogs.microsoft.com/on-the-issues/2022/04/07/cyberattacks-ukraine-strontium-russia/.

[79] Ibid.

panies will offer their services to the highest bidder, much like NSO Group. Any hacker or researcher with sufficient knowledge can look for zero days and develop exploits. Although these vulnerabilities are regularly sold in online black markets, coalescing them in corporations makes it easier and cheaper to purchase them. Mercenary companies will also focus on upgrading espionage software to hack into devices. Espionage would not only be used to steal secrets for blackmail or intellectual property theft, but it can also serve as the basis for targeting potential threats. A possible scenario is that a company like NSO Group creates software to break into phones more efficiently, then China uses it to locate and neutralize CIA agents throughout Asia.

"The United States has a long history of working with corporations to achieve its security and strategic interests, but it will have to find a balance when its interests diverge from those of corporations."

A country's relative balance of power is likely to be intimately connected to native technology companies as they become essential to economic growth and defense of infrastructure and businesses, participate in investigations and attributions, and even engage in offensive operations. Recent trends and changes in how countries in Asia manage their technology companies indicate that the balance of power will probably shift toward middling powers. There would be less interdependence and more conflict.

Implications for U.S. Strategic Interests and Competition

The United States will probably have a more favorable position in Asia in coming decades because of the likely changes in the Asian balance of power, which may be marked by more conflict and less interdependence due to multinational tech companies. Technonationalist tendencies in places like Japan might mean countries will only want to work with trusted partners, and U.S. technology companies are more likely to be trusted partners because they have a long history of working with foreign partners. In addition, U.S. venture capital firms will probably have more access to countries that deny access to China. U.S. corporations already have an advantage from having worked closely with the government on national security matters. Microsoft, Google, Amazon, Meta, etc. all have the infrastructure to target threat actors online, whether they are substate or state actors. Government agencies like the NSA have a large network from which they can purchase zero-day vulnerabilities and other kinds of software for espionage. The United States could also benefit from minor issues like data analysis, artificial intelligence, and OSINT. Government agencies work with technology companies on multiple levels, from analytic exchange programs to tech executives working in the government.

The primary challenge for the United States over the coming decades will be to maintain a relationship with its own private sector technology companies in which the federal government maintains control over strategic priorities. The United States has a long history of working with corporations to achieve its security and strategic interests, but it will have to find a balance when its interests diverge from those of corporations that take on some core functions of security. Those relationships have been a key variable in the United States winning against peer competitors and remaining a great power for more than a century. After 9/11, the nature of transnational terrorist networks and their ability to strike globally led to a dilemma in which the American approach to war needed even better technological tools. To achieve their goals, the U.S. government turned to Silicon Valley, but this was different than during the Cold War. As Margaret O'Mara noted, "Instead of government-funded academic labs and contracts producing military tech that later could be commercialized, now the defense establishment created VC [venture capital] firms to seed private software companies that could one day become contractors."[80] This has led to major contracts with technology companies that have allowed the United States to keep its competitive edge.

One area in which the United States is ahead of other countries is its willingness to use corporations to target threat actors, even those that do not threaten governmental institutions. For example, in June 2013, Microsoft led Operation b54 to bring down Citadel, a cybercrime group that had infected thousands of machines worldwide for use as an army of botnets.[81] Microsoft, with the support and help of nine financial institutions, severed the lines of communication between the botnets and took control of servers used in malicious attacks. There are dozens of examples along these lines. Even though Microsoft has been one of the most prolific partners in these efforts, they have not been the only one. Relationships have been developed with Mandiant, FireEye, and other tech companies to bring down the infrastructure of threat actors. The United States will have a strong position in this competition if they are able to keep these relationships strong and productive, which would give the United States a better position in Asia. Several Asian countries, such as Vietnam, China, and North Korea, have a significant number of threat actors that target U.S. corporations. Having technology and cybersecurity corporations prepared to defend against those threat actors will make the United States much stronger in the region.

[80] Margaret O'Mara, *The Code: Silicon Valley and the Remaking of America* (New York: Penguin Press, 2019), 384.

[81] Harris, *@War*, 118.

Security and capital investments have kept the relationships good between the government and corporations, but political movements in the United States have become hostile toward Big Tech, which could undermine the needed connection. Left-wing politicians believe these companies contribute to inequality, while right-wing politicians blame technology companies for censorship. This has led to antimonopoly efforts in Congress, multiple hearings involving tech executives, and pro-regulation proposals in the executive branch. If the U.S. government chooses an antagonistic approach to tech companies, then it may lose its favorable position in Asia over the next two decades. This would significantly harm economic growth. Research into the kind of technology, software, and innovative practices needed for more growth in the United States cannot come from smaller companies or even the government. Defense contracts, though lucrative, are not as profitable or necessary as they were decades ago because of venture capitalist firms. Only Big Tech can research areas that are not immediately profitable. More regulations could harm the United States' economic interests. In addition, U.S. technology companies as they currently exist are the only ones with the resources, infrastructure, and technical know-how to play the kind of role needed in national security and defense. Companies like Microsoft can target Chinese threat actors because of their resources. Antimonopoly efforts would denude tech companies of that ability, while countries that take a more collaborative approach to working with technology companies would gain advantages over the United States.

Therefore, over the coming decades, the United States may gain in the relative balance of power because its existing relationship with technology companies gives it access to more revenue, economic growth, defensive capabilities, and offensive operations. What the United States decides to do about technology companies over the next two decades will determine whether that is the most likely path. Technology companies are now one of the most important factors in U.S. strategic, economic, and security interests, and they are the basis for a country's place in the balance of power.

Conclusion

Technology and the companies that develop it impact practically every aspect of modern existence—travel, communication, financial transactions, energy, social media, and healthcare, to name just several. These companies now operate as part of national security by protecting customer data, physical infrastructure, and social institutions; directly targeting threat actors; and collecting intelligence on threats. These companies sometimes even participate directly in conflict or use offensive actions to protect their customers. With tech companies taking on important security roles traditionally handled by states, they may reconfigure the balance of power in Asia. This paper has evaluated aspects of the core state function of security to which tech corporations have contributed and explored aspects of a plausible future. These include:

- **The role corporations have played in intelligence gathering and covert operations to support the state**. China is likely to use corporations for these purposes, which are historically taken on by states. This would take place because of regulations that would encourage the state and corporations to engage in more covert operations. Those same regulations would encourage technological development in other countries. Middling powers may then have greater defense capabilities and power projection because of economic development from technology corporations, and countries like Indonesia can use tech corporations to increase their power relative to other states.
- **How the structure of the internet and regulations will determine economic growth and power.** Regulatory changes and a balkanized internet may be brought about by security concerns, such as Japan's possible security law or Western countries blocking Chinese corporations. Internet blocs may form in response, and countries may be forced to choose which bloc to join for economic development. Corporations would be an important foundation for power projection in this scenario, and balkanization would probably increase the likelihood of attacks by state actors because there would be a reduced risk of blowback or indirect harm to their networks.
- **The role of corporations in conflict, both as targets and attackers.** This has already occurred in geopolitical disagreements between China and India and China and Australia. Corporations could be a critical part of power projection or become a new defense industry base. The Russia-Ukraine war is an example of a path this could take in Asia.

The phenomenon of corporations taking on aspects of the core state function of security better defends data, supports the targeting of threat actors, and supplies offensive capabilities, but there are concerns about how the state can control corporations' behavior and be sure to partner only with those that support the common good. This is not a new issue. Niccolò Machiavelli, the sixteenth-century political theorist and diplomat, expressed negative views about private actors in security in *The Prince.* Machiavelli called them "useless and dangerous" and advised princes not to use their services in conflict because "there is no loyalty or inducement to keep them on the field apart from the little they are paid."[82] Machiavelli feared that craven and selfish actors would not work for the common good. Rather, these private entities would use their powers for nefarious purposes, cravenly back down from sophisticated threats, or refuse to help protect the country because there was no profit. If one accepts that technology corporations will take on security functions, there must be further ethical, political, and strategic assessments by scholars, practitioners, and policymakers that develop mechanisms or protocols to have corporations provide security for the common good.

Determining how governments interact with, coopt, or partner with corporations will only be the start. Further research on security implications will be needed because corporations taking on core state functions in security may

[82] Niccolò Machiavelli, *The Prince* (New York: Penguin Books, 1995), 38.

impact more than governance strategies. For example, the determinants of power could fundamentally change over the coming decades, and corporations could take on a central role in governance itself. Corporations could even start a war if they choose to respond offensively to state aggression; some states have looked at potential hack back legislation that would allow companies to target threat actors outside the country's borders.[83] Corporations could also change the nature of alliances, becoming the determining factor in how countries work with each other. To a small extent, some corporations already participate in global diplomacy on technology issues, such as Microsoft advocating for the Digital Geneva Convention. If corporations become the central feature of alliances or participate in governance, this could also change constituencies or constitutional structures. It is conceivable that under this shift, corporations could gain voting or participation rights, if not in the domestic sphere then at international organizations like the United Nations or NATO.

There should also be further study into how technology companies and other multinational corporations are taking on the other two core functions of the state: revenue mobilization and adjudication of disputes. This development is already taking place in cases such as tax preparation, cryptocurrency companies, private prisons, and facial recognition. Even though corporations contributing to the core state function of security is beneficial, the same benefits might not be derived in other areas. These changes in the role of corporations could alter most aspects of society, politics, economics, diplomacy, and warfare—each shift requires its own exploration and research. This paper is only the start of understanding the new role of corporations in geopolitics and how it may reconfigure the Asian balance of power. It will take significantly more work over the coming years by government, academic, and private sector researchers to fully elucidate the possibilities and implications.

[83] The Active Cyber Defense Certainty Act (ACDC) that would allow hacking back has been introduced several times in the U.S. Congress, though it has never passed. In addition, active cyber defense was discussed at the European Parliament on the draft of the Network and Information Security Directive (NIS 2 Directive).

The Andrew W. Marshall Foundation

Founded by Andrew W. Marshall and Jaymie Durnan, with the continued support of generations of people who worked for, worked with, or were mentored by Andy Marshall, the Andrew W. Marshall Foundation is a 501(c)(3) tax-exempt organization. The people and work it supports are impartial and intellectually fearless.

Designed by: Selena Robleto, Red Velvet Creative

Edited by: Thomas Mowle, Rampart Professional Solutions

The Andrew W. Marshall Foundation
1 Woodbury Hill Road
Jaffrey, NH 03452
www.andrewwmarshallfoundation.org