



Submarine Cables and Container Shipments: Two Immediate Risks to the US Economy if China Invades Taiwan

Christine McDaniel and Weifeng Zhong

August 2022

One uncertainty facing the global economy is whether there will be a geopolitical incident in the Taiwan Strait. An outright invasion of Taiwan by China, a Taiwanese declaration of independence, or an accidental clash at sea between China and Taiwan or the United States—any of these developments could lead to a crisis in the Taiwan Strait, which would pose two immediate risks to the US economy: (a) potential disruptions to digital flows from vulnerable submarine cables with landing stations in Taiwan and (b) the delay or disruption of container shipments in the Taiwan Strait, South China Sea, and East China Sea on their way to or from the United States.

Trade and economic effects of a Chinese invasion of Taiwan could easily exceed those of Russia's invasion of Ukraine. The economies of China and Taiwan are much larger than those of Russia and Ukraine (China's economy is about 10 times larger than Russia's, and Taiwan's is about 4 times larger than Ukraine's), and the exposure of the US economy to China and Taiwan is far greater, not only in trade volumes but also in the share of value the two countries add in US final demand. Taiwan also has an outsized role in the global advanced semiconductor chip industry, and disruptions to the supply of these chips or to US companies' digital communications with Taiwanese partners would unsettle the US tech sector and nearly every industry that uses advanced computer chips.

China's military, the People's Liberation Army (PLA), appears to have planned extensively for invasion scenarios.¹ Our analysis of open-source data reveal China's strategic points of interest: locations of economic importance, potential military locations, and key digital infrastructure such as submarine cable landing stations.²

Ocean routes for the transport of goods in container ships are easy to find. But the infrastructure for digital flows (the undersea cable network) is less conspicuous. Hundreds of thousands of miles of cable line the ocean floor, connecting to land-based stations with power and networking infrastructure to facilitate reliable intercontinental communications. Nearly all digital and internet traffic relies on submarine cables. If a cable is cut or a landing station is damaged (intentionally or not), the flow of those data is directly affected.

Compared with the effects of Russia's invasion of Ukraine, the stakes of a Taiwan Strait crisis are greater for the US economy, with a heightened risk to US goods trade and digital flows. The economic risks underscore the need for the United States to work with Taiwanese authorities and other Indo-Pacific allies and partners to improve the security of submarine cables and their landing stations, as well as the need for contingency planning for container shipping traffic and essential intermediate inputs to US production and value chains.

We do not consider the possibility of economic sanctions in this brief, such as Western sanctions on China or potential countersanctions by Beijing on the West, or the possibility of involvement from other great powers. In the event of sanctions or wider conflicts, costs for the US economy would go beyond disruptions to container shipping—or loss of ships—and digital flows. We view the scenarios discussed in this brief to be on the lower end of the spectrum in terms of intensity or severity.

OPEN-SOURCE DATA ILLUSTRATE PRESSURE POINTS

China has long been known to have ambitions for taking over Taiwan, and it has stated repeatedly that it would not rule out doing so by force.³ PLA planning for invasion scenarios appears to be extensive and includes a wide range of detailed strategies. Public information on how such a take-over would unfold and how Taiwan's economy and territory might be vulnerable is scant, however.⁴

We present new evidence from New Kite Data Labs that sheds light on locations, or points of interest (POIs), in Taiwan that may be strategic priorities for China economically or militarily (or both). This evidence may indicate the kind of documentation PLA is gathering, and it underscores the risks to US goods trade and digital trade with and through Taiwan in the event of a crisis in the strait.

This new evidence is a database left unguarded at a Chinese internet protocol (IP) address and obtained by New Kite Data Labs in April 2021. The IP address is owned by Hangzhou Alibaba Advertising Co. Ltd., a fraudulent internet service provider operating over a million IP addresses for third-party users.⁵ According to information provided to us by Breadcrumb Cybersecurity acquired using open-source intelligence platforms, this IP address was associated with multiple malicious cybersecurity incidents between August 2019 and October 2021 targeting the United States.⁶ These incidents include Mirai malware attacks performing command and control protocols on its targets.⁷

The database contains 294,100 POIs in Taiwan, each with latitude, longitude, postal address, and telephone number, among other information. In addition, 96 percent of the locations are labeled by type. These types vary widely and include restaurant, barber shop, school, road intersection, government building, and military camp.

Some POIs, such as offices of companies in the software industry, are likely of interest to the Chinese entity as business intelligence; they could be relevant to Chinese companies doing business in Taiwan and, hence, competing with them. But other POIs, such as military facilities and public infrastructure, are more likely to be of military interest because those locations are strategically important and vulnerable in a kinetic conflict. We focus on the latter and visualize them on the map of Taiwan in figure 1.

First, there are 183 military POIs (see panel A), such as military bases, military schools, and military camps. Examples include the Republic of China Navy's Haifeng Brigade, an ammunition depot in Cishan (near Kaohsiung), the Republic of China Military Police Command headquarters, and the Army Logistics Training Center.

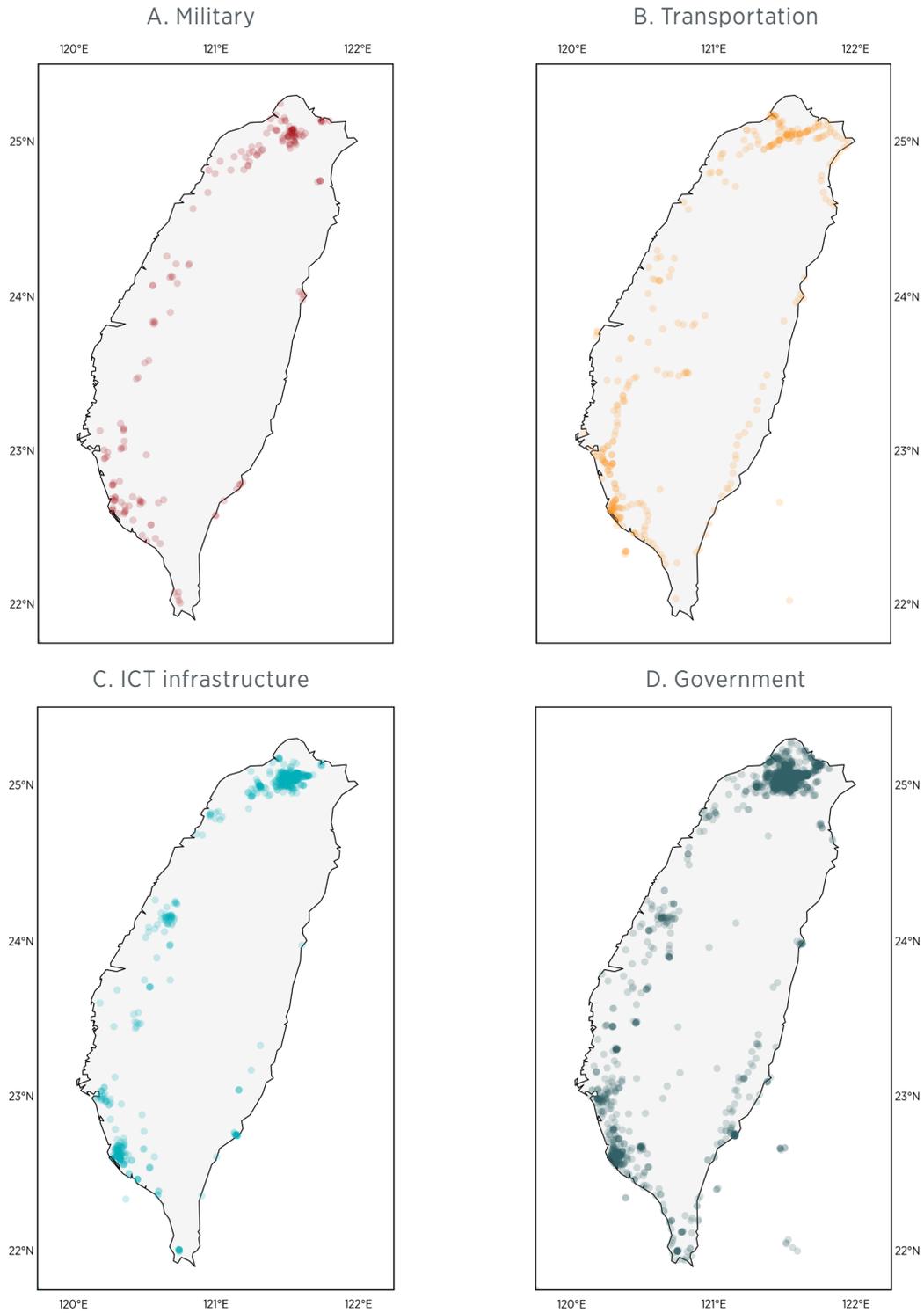
Second, there are 341 transportation POIs (see panel B), such as airports, train stations, and seaports. Examples include the Taoyuan International Airport, the Taichung station of the Taiwan High Speed Rail and the Port of Kaohsiung.

Third, there are 550 POIs related to information and communication technology (ICT) infrastructure (see panel C), such as telecommunication facilities and internet service provider facilities (e.g., submarine cable landing stations). Examples include Chunghwa Telecom's various facilities, Taiwan Mobile's various facilities, Qualcomm Taiwan Corporation headquarters, and other ICT service provider offices.

Fourth, there are 2,397 government POIs (see panel D), such as government agencies and buildings from the national and provincial levels to the township and village levels. Examples include the National Security Bureau (Taiwan's principal intelligence agency) and a village government office on Orchid Island (east of the main island of Taiwan).

The POIs are comprehensive, and their locations are spread across Taiwan's territory, including in areas that are sparsely populated. The data suggest that at least one Chinese entity, possibly a government-affiliated entity, is paying close attention to a variety of economically and militarily critical locations on the island.

Figure 1. Points of Interest in Taiwan Curated by a Chinese Entity



Note: ICT = information and communication technology.
Source: New Kite Data Labs, email messages to authors, n.d.

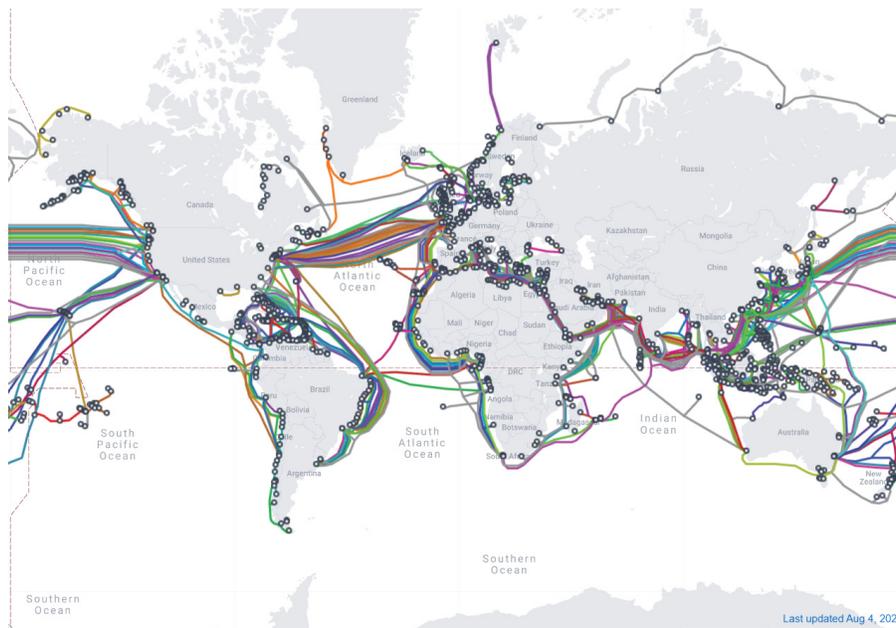
SUBMARINE CABLES IN THE DIGITAL ECONOMY

People’s day-to-day lives increasingly rely on wireless connectivity, but the bedrock of the internet is submarine cables lining the ocean floor.⁸ The history of submarine cables goes back to the 1820s, when the first cables were used to send an electric telegraph from the Russian embassy in Munich.⁹ Today there are over 450 cables across the ocean floor and over 1,300 unique coastal landing stations (see figure 2). These sophisticated fiber-optic cables are responsible for transmitting nearly all transoceanic data and digital communications such as phone calls, emails, and web pages.

Despite their vital role in the digital economy, submarine cables are surprisingly vulnerable, and the rules that provide their security are outdated.¹⁰ The most obvious threats are physical, given that submarine cables can be damaged in many ways: bitten by sharks, hit by ship anchors, shaken by earthquakes, sabotaged by malicious actors, etc.¹¹ In 2018, a cable connecting West Africa’s coast to Europe was cut for some unknown reason, affecting six African countries that relied entirely on that one cable for their connectivity to the submarine cable network.¹² The 2011 Tōhoku earthquake and tsunami damaged about half of the cables running across the Pacific and disrupted internet connectivity in Japan and elsewhere in Asia.¹³

Submarine cables come to shore at landing stations that are critical infrastructure for the network. These stations are not always conspicuous, and a typical landing station often does not look that different from any other small building (see figure 3).

Figure 2. Submarine Cable Map as of August 2022



Source: “Submarine Cable Map,” TeleGeography, last updated August 4, 2022, <https://www.submarinecablemap.com/>.

Figure 3. A Cable Landing Station in Toucheng, Taiwan



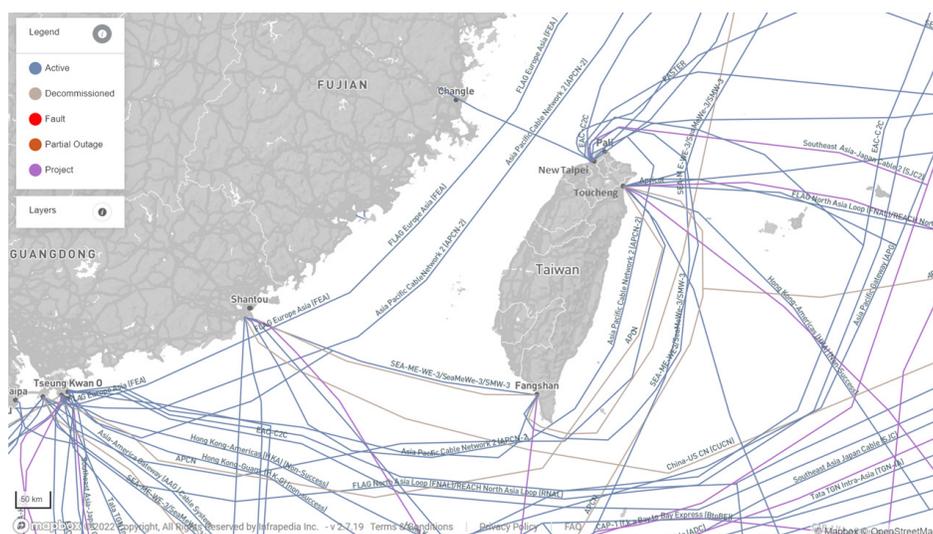
Source: "Google Maps," Google, accessed August 10, 2022, <https://goo.gl/maps/NJQfMhxeKDMszbZY6>.

As of August 2022, Taiwan was connected to 15 submarine cables, which come to shore at landing stations in just three areas: the city of New Taipei, the town of Toucheng in the north, and the town of Fangshan in the south (see figure 4). These landing stations connect high-capacity cables in which US technology companies have made significant investment. For instance, the Pacific Light Cable Network is owned by Google and Meta and became ready for service in January 2022. The network, which is protected through advanced encryption, has landing points in Toucheng, Taiwan; Baler, Philippines; and El Segundo, California.¹⁴ One of Taiwan's landing stations in Tanshui (part of New Taipei) is an ICT infrastructure POI tracked by the Chinese entity referenced in the previous section, suggesting that the vulnerability of submarine cable infrastructure on the island is relevant.

The lack of protection by international law exacerbates cable vulnerabilities. According to James Kraska at the US Naval War College, the principal treaties governing submarine cables are the 1884 Convention for the Protection of Submarine Telegraph Cables, the 1958 Convention on the Continental Shelf, and the 1982 United Nations Convention on the Law of the Sea. These instruments provide some—if outdated—peacetime protection to submarine cables. During open conflicts, however, the applicability of these rules is questionable, and Kraska notes that, in practice, cables connecting two points in enemy territory may be cut.¹⁵

The economic cost of a disruption to digital communications is not clear. Some researchers have attempted to estimate the contribution of the internet to the global economy.¹⁶ One report estimates that the daily effect of a temporary shutdown of the internet and all of its services for a highly connected country is approximately \$23.6 million per 10 million people.¹⁷ Given Taiwan's

Figure 4. Submarine Cables Connecting Taiwan as of August 2022



Source: Infrapedia (website), accessed August 10, 2022, <https://www.infrapedia.com/app>.

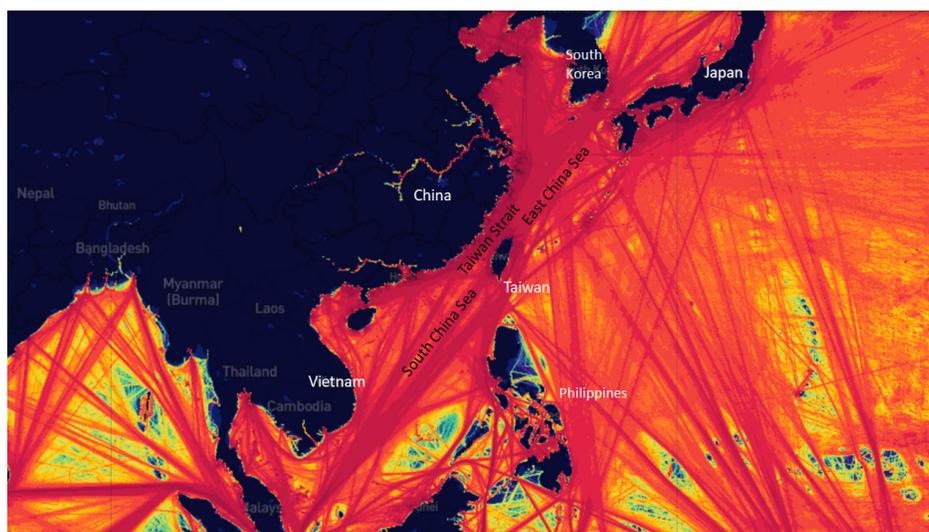
population of 23.57 million, the average cost would work out to \$55.63 million per day or \$1.69 billion per month. The economic effects over time would not be linear, however, and the costs of disruption would quickly escalate if companies were compelled to make larger production adjustments during a sustained conflict.¹⁸

CONTAINERIZED SHIPMENTS IN THE TAIWAN STRAIT

The South China Sea is one of the world’s busiest sea routes. Estimates are that \$3.4 trillion in trade passed through the South China Sea in 2016, or 21 percent of the global trade in that year.¹⁹ The South China Sea is connected by the Taiwan Strait with the East China Sea, which meets South Korea and Japan, and by the Luzon Strait with the Philippine Sea. Figure 5 shows the vessel density in and around the South China Sea, the Taiwan Strait, and the East China Sea.

The disruption from a crisis in the Taiwan Strait could affect containerized shipments to or from major ports in China, Japan, the Philippines, South Korea, Taiwan, and Vietnam. Such a disruption has occurred with the Russian invasion of Ukraine, which insurance data suggest has caused significant decline in Black Sea traffic. For instance, according to Bloomberg, in April 2022, a \$50 million, five-year-old tanker hauling a standard one million barrels of Russian cargo would need to pay \$5 million just in war-risk premium to sail in the Black Sea—about \$1.5 million greater than the cost of hiring the carrier. Yet before the invasion, such insurance cost practically nothing.²⁰ Similar war-risk premiums would be likely for other types of air and shipping cargo.

Figure 5. Sea Route Density Map of 2021



Note: Darker shades of red indicate more traffic.

Source: MarineTraffic (website), accessed August 10, 2022, <https://www.marinetraffic.com/>.

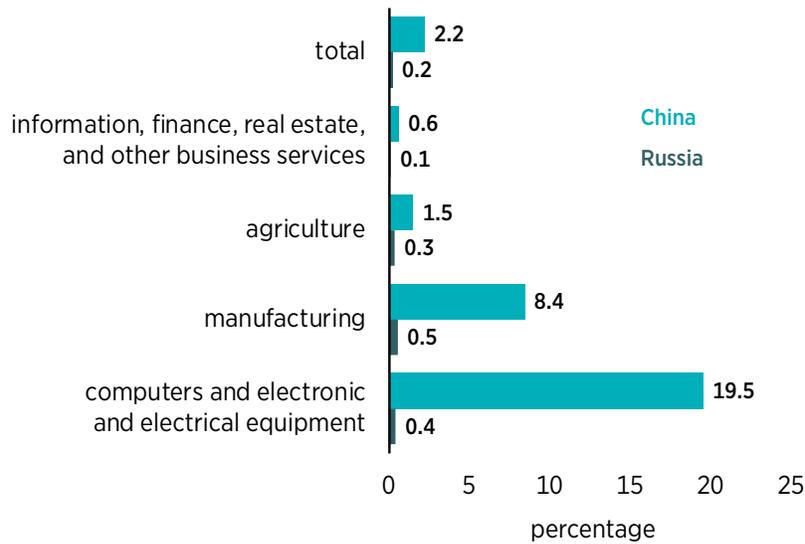
US production is more reliant on China and Taiwan for intermediate inputs than on Russia and Ukraine. Data from the Organisation for Economic Co-operation and Development on value added in US final demand indicate that China accounts for 2.2 percent and Russia accounts for 0.2 percent (see figure 6). For imported intermediate inputs, China accounts for 17.8 percent of US final demand and Russia accounts for 1.5 percent (see figure 7). The heavy reliance on China is starker in manufacturing, and even more so in computers and electronic and electrical equipment.²¹

Rerouting Costs

In the event of a crisis, shipping routes that would normally go through the Taiwan Strait could be delayed, rerouted, or both, and this could affect US trade with at least China, Japan, the Philippines, South Korea, and Vietnam, let alone Taiwan. Rerouting to avoid the war-risk premium would be possible but not costless. If the crisis were contained, existing traffic in the Taiwan Strait could be rerouted to the waterways to the east of the island, but doing so would lengthen shipping times. For instance, one of the busiest shipping routes is in the Straits of Malacca, given that it is the shortest sea route between the Indian and Pacific oceans. Costs of rerouting all traffic around the Straits of Malacca have been estimated between \$279 million per month (if rerouting through Indonesia) and \$2.82 billion per month (if rerouting through Australia).²² Actual costs would depend on the length of the disruption and whether energy shipments were affected.

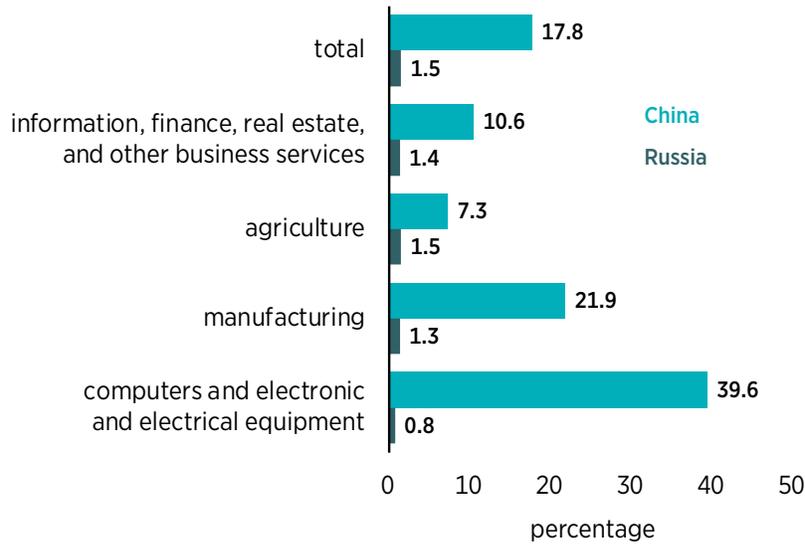
The geographic reach of a crisis that starts in the Taiwan Strait may not be limited to the strait. If US, Chinese, and possibly Japanese fleets end up exchanging missile and torpedo fire, then

Figure 6. Share of Chinese and Russian Value Added in US Final Demand



Source: Organisation for Economic Co-operation and Development, Trade in Value Added (database), 2021 ed., November 12, 2021, <https://www.oecd.org/sti/ind/measuring-trade-in-value-added.htm>.

Figure 7. Share of Chinese and Russian Imported Value Added in US Final Demand



Source: Organisation for Economic Co-operation and Development, Trade in Value Added (database), 2021 ed., November 12, 2021, <https://www.oecd.org/sti/ind/measuring-trade-in-value-added.htm>.

the geographic reach of the crisis could extend to the farther reaches of the Western Pacific (i.e., South China Sea, East China Sea, Sea of Japan, Philippine Sea) and through the Luzon Strait, which is a key shipping and communications route for the Americas. Any geographic expansion of a crisis that begins in the Taiwan Strait would easily make rerouting harder, if not impossible.

Delays

Economists often measure the costs of shipping delays in terms of an ad valorem tariff. Each day of shipping delay is an estimated 1 percent to 2 percent ad valorem tariff equivalent.²³ Hence, for standard ex ante analysis, the cost of a one-week delay would be equivalent to 7 percent to 14 percent of the customs value of trade flows that go through the disrupted routes. But as the past two years have shown, the economic effects of a delay of a critical component or highly specialized machinery extend beyond the payment of a simple import tax. For instance, the global auto industry cut back production in 2021 owing to computer chip shortages.²⁴

The delay of essential components can easily translate into a production stoppage once backup inventory runs out. Many major US technology firms reportedly rely on Taiwanese manufacturers to produce up to 90 percent of semiconductor chips.²⁵ Disruptions to the supply of these chips or the ability to digitally communicate with Taiwanese chipmakers would propagate throughout the entire value chain ecosystem for every US industry that uses advanced computer chips (e.g., electronics, computers, and smartphones). Researchers interested in estimating economy-wide or sector-specific potential economic effects of container shipment delays may need to look beyond standard analytical approaches.

Loss of Container Ships

A grimmer possibility is the loss of container ships in the Taiwan Strait and nearby routes in the South China Sea or East China Sea. Such a loss could occur if those ships are sunk by PLA naval submarines imposing a hard blockade on Taiwan or if US or Chinese missiles hit a commercial ship. And although missile targeting technology is sophisticated, existing research and recent events suggest misses do happen, leaving the odds of an accidental hit a commercial consideration.²⁶

CONCLUSION

The potential effects of a Chinese invasion of Taiwan on the US economy are far greater than those of the Russian invasion of Ukraine. Container shipments to and from major ports in the region, as well as digital flows, would be at direct risk. China and Taiwan are also major suppliers and consumers for US major trading partners around the globe from Japan and Germany to Saudi Arabia. The effects of a crisis or blockade would be felt by every major economy, which, in turn, would produce additional negative effects for the US economy.

The bedrock of the internet is the submarine cables lining the ocean floor, and new evidence reveals the points of interest for China, which include economic centers, potential military locations, and submarine cable landing stations. This evidence portends a heightened risk to US goods trade and digital flows with and through Taiwan, should there be a crisis in the Taiwan Strait.

This brief highlights the need for the United States to work with Taiwanese authorities and other Indo-Pacific allies and partners to improve security for submarine cables and their landing stations, as well as engage in contingency planning for container shipping traffic and essential intermediate inputs to US production and value chains.

ACKNOWLEDGMENT

We are grateful to Bruce Jones for his extremely valuable comments on this brief and to Jim Ronyak and Brian Horton for providing illuminating information about the Chinese threat actor mentioned in this brief.

ABOUT THE AUTHORS

Christine McDaniel is a senior research fellow at the Mercatus Center at George Mason University. Her research focuses on international trade, globalization, and intellectual property rights. McDaniel previously worked at Sidley Austin, LLP, a global law firm, where she was a senior economist. She has held several positions in the US government, including deputy assistant secretary at the Treasury Department and senior trade economist in the White House Council of Economic Advisers, and she has worked in the economic offices of the US Department of Commerce, US Trade Representative, and US International Trade Commission.

Weifeng Zhong is a senior research fellow at the Mercatus Center at George Mason University. Zhong has a PhD in managerial economics and strategy from Northwestern University. His work focuses on bridging the field of natural language processing and machine learning to economic policy studies. He is also a core maintainer of the open-source Policy Change Index, a machine learning framework to predict policy changes in authoritarian regimes.

NOTES

1. John Grady, "Panel: China Planning a 'Go Big, Go Early' Strategy Against Taiwan," *USNI News*, April 14, 2022.
2. The term "open-source" in the context of data or intelligence refers to information and analysis of data gathered from public domains.
3. "LIVE: 40th Anniversary of 'Issuing Message to Compatriots in Taiwan,'" policy speech by Chinese President Xi Jinping, CCTV Video News Agency, January 1, 2019, <https://www.youtube.com/watch?v=not9jASVHds>.
4. The Gaming Lab at the Center for a New American Security recently released a report on a high-level strategic-operational wargame exploring a fictional war over Taiwan set in 2027. Stacie Pettyjohn, Becca Wasser, and Chris Dougherty, *Dangerous Straits: Wargaming a Future Conflict over Taiwan* (Washington, DC: Center for a New American Security, 2022).
5. "Hangzhou Alibaba Advertising Co. - Fraud Risk," Scamalytics, accessed August 18, 2022, <https://scamalytics.com/ip/isp/hangzhou-alibaba-advertising-co>.

6. "FILEHASH - SHA256 0eeb381512ece45e6faa308c7d62288e176b00a7fc5831e3c685139473d09c64," Alien Vault, accessed August 18, 2022, <https://otx.alienvault.com/indicator/file/0eeb381512ece45e6faa308c7d62288e176b00a7fc5831e3c685139473d09c64>.
7. Unfortunately, we do not have enough evidence to determine the identity of the Chinese threat actor.
8. Bruce D. Jones, *To Rule the Waves: How Control of the World's Oceans Shapes the Fate of the Superpowers* (New York: Scribner, 2021).
9. Lionel Carter et al., *Submarine Cables and the Oceans: Connecting the World* (Cambridge, UK: United Nations Environment Programme World Conservation Monitoring Centre, 2009), 11.
10. Karen Scott, "Laws Governing Undersea Cables Have Hardly Changed since 1884—Tonga Is a Reminder They Need Modernising," *The Conversation*, January 20, 2022; Nicholas Kazaz, "Are Laws Regulating Subsea Cables Outdated?," *Submarine Telecoms Forum*, March 29, 2022.
11. Submarine cables also face digital vulnerabilities, such as being tapped by adversaries. US and UK intelligence agencies reportedly have performed such operations for decades. In recent years, Russia has intensified its submarine activity around undersea cables, and observers suggest that it may have similar capability to tap them. Although cable tapping may have indirect economic consequences (e.g., through compromising intelligence), this brief focuses on the direct effects of physical disruptions to Taiwan's cables.
12. Russell Brandom, "A Broken Submarine Cable Knocked a Country Off the Internet for Two Days," *The Verge*, April 8, 2018.
13. Owen Fletcher and Juro Osawa, "Rush to Fix Quake-Damaged Undersea Cables," *Wall Street Journal*, March 15, 2011.
14. "PLCN," Submarine Cable Networks, accessed August 10, 2022, <https://www.submarinenetworks.com/en/systems/trans-pacific/plcn>. Initially, the plan was to include a landing station in Hong Kong, but US security agencies asked the Federal Communications Commission to deny the link to Hong Kong because it would give China a way to acquire personal data on millions of Americans.
15. James Kraska, "Submarine Cables in the Law of Naval Warfare," *Lawfare* (blog), July 10, 2020.
16. Broadband internet accounted for 72 percent of the total revenue in internet access in 2006. Shane Greenstein and Ryan C. McDevitt, "The Broadband Bonus: Accounting for Broadband Internet's Impact on U.S. GDP" (NBER Working Paper No. 14758, National Bureau of Economic Research, Cambridge, MA, February 2009). A 2011 report by McKinsey estimates that the internet accounted for 21 percent of GDP growth in mature economies from 2005 to 2010, and it notes that if the internet were a sector, it would have a greater weight in GDP than agriculture or utilities. James Manyika and Charles Roxburgh, *The Great Transformer: The Impact of the Internet on Economic Growth and Prosperity* (New York: McKinsey Global Institute, 2011).
17. Deloitte, *The Economic Impact of Disruptions to Internet Connectivity*, 2016.
18. Disruptions to digital flows might be a negative shock to productivity. The magnitude of the shock is far from clear, but the Organisation for Economic Co-operation and Development (OECD) estimates that over half of productivity comes from ICT. Specifically, the estimated ICT contribution to total factor productivity is 59.0 percent for the United States and 100.0 percent for Japan, whereas the average among OECD countries was 57.9 percent (Taiwan is not included in the OECD's analysis because it is not a member). Vincenzo Spiezia, "ICT Investments and Productivity: Measuring the Contribution of ICTs to Growth," *OECD Journal: Economic Studies* 2012, no. 1 (2012): 209; authors' calculations.
19. "How Much Trade Transits the South China Sea?," ChinaPower, Center for Strategic and International Studies, last updated January 25, 2021, <https://chinapower.csis.org/much-trade-transits-south-china-sea/>.
20. Ann Koh and Alaric Nightingale, "The Cost of Insuring Black Sea Shipping Is out of Control," *Bloomberg*, April 8, 2022.
21. Taiwan accounts for 0.18 percent of value added in US final demand and 1.48 percent of imported value added in US final demand. For the computers and electronic and electrical equipment sector, the figures are 2.12 percent and 4.31 percent, respectively. Data for Ukraine are not available. Organisation for Economic Co-operation and Development, *Trade in Value Added* (database), 2021 ed., November 12, 2021, <https://www.oecd.org/sti/ind/measuring-trade-in-value-added.htm>.

22. "How Much Trade Transits the South China Sea?"
23. David L. Hummels and Georg Schaur, "Time as a Trade Barrier," *American Economic Review* 103, no. 7 (2013): 2935–59.
24. AlixPartners (website), accessed August 10, 2022, <https://www.alixpartners.com/>.
25. Saheli Roy Choudhury, "Tough Road Ahead for U.S. Firms Trying to Cut Reliance on Taiwan Chipmakers," CNBC, April 13, 2021.
26. T. S. Gokkul Nath, P. Sudheesh, and M. Jayakumar, "Tracking Inbound Enemy Missile for Interception from Target Aircraft Using Extended Kalman Filter," in *Communications in Computer Information Science*, ed. Amin Mobasheri, vol. 625, *Security in Computing and Communications*, ed. Peter Mueller et al. (Jaipur, India: Springer Nature Singapore, 2007). A recent Chinese hypersonic missile missed by "about two-dozen miles." Demetri Sevastopulo and Kathrin Hille, "China Tests New Space Capability with Hypersonic Missile," *Financial Times*, October 16, 2021. Meanwhile, Russia has had an estimated 60 percent miss rate. Phil Stewart, "Exclusive: U.S. Assesses up to 60% Failure Rate for Some Russian Missiles, Officials Say," *Reuters*, March 25, 2022.