



| Flash |

Chinese Threat Actors Targeting Philippines over Sea Disputes

F-2024-02-09b

Classification: TLP:CLEAR

Criticality: Medium

Intelligence Requirements: Geopolitical, Supply Chains

February 9, 2024

Scope Note

ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were **identified prior to 10:00 AM (EST) on February 9, 2024**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Flash | Chinese Threat Actors Targeting Philippines over Sea Disputes

> Key Findings

- China is likely escalating its military and cyber activity against its neighbors to project power in disputed waters.
- Philippines defense officials claim to have thwarted attempts from China-backed hackers to break into government websites and email systems. ZeroFox also identified cyber threat actors targeting a Philippines-based shipping company.
- Tensions have been rising, with repeated confrontations between Chinese and Philippine vessels in the South China Sea. China is engaged in similar territorial disputes with several of its other neighbors, all of which have established closer ties with the United States in recent years.
- A key trade agreement between the United States and Pacific nations that isolates China is due to go into effect in late February 2024.
- With an increasing number of its neighbors rejecting China's claims to the expansive South and East China Sea territories, expect further Chinese efforts to undermine their governments.

Details

China is likely escalating its military and cyber activity against its neighbors to project power in disputed waters. Recent Chinese activity has been directed towards the Philippines, with tensions rising amidst repeated confrontations between Chinese and Philippine vessels in the South China Sea. China is engaged in similar territorial disputes with several of its other neighbors, all of which have established closer ties to the United States in recent years.

- Of all the waters claimed by China, those near the Philippines are arguably the most important. The Philippines' geographic location would allow it to limit China's access to the maritime supply chains that its export-dependent economy needs. During a war, U.S. bases on the island could be used to target China.
- To project power in the disputed territory, China will likely escalate its cyber and military activity.

This escalating activity has now spread to include offensive cyber campaigns. On February 5, 2024, the Philippines' Department of Information and Communication Technology (DICT) announced that it had thwarted attempts from China-backed hackers to break into the Philippine Coast Guard (PCG)'s websites, as well as the email systems of the president and government agencies.

- DICT said these breaches targeted critical domains such as cabsec[.]gov[.]ph, coastguard[.]gov[.]ph, cpbrd.congress[.]gov[.]ph, dict[.]gov[.]ph, doj[.]gov[.]ph, and ncws[.]gov[.]ph; based on the internet protocol addresses, the hackers appear to be using the services of Chinese state-owned telecommunications company Unicom.¹
- Chinese-backed threat activity against Philippine government websites is very likely linked to its ongoing territorial dispute with the Philippines in the South China Sea.

China has aspirations to become a military and economic superpower that can outmaneuver the United States. To do so, it needs secure access to the Pacific Ocean to

¹

[hXXps://ciso.economictimes.indiatimes\[.\]com/news/cybercrime-fraud/philippines-wards-off-cyber-attacks-from-china-based-hackers/107445842](https://ciso.economictimes.indiatimes.com/news/cybercrime-fraud/philippines-wards-off-cyber-attacks-from-china-based-hackers/107445842)

support its export-dependent economy and the ability to withstand and launch military aggression by sea. However, a slew of U.S. allies that host U.S. military bases claim many of the same waters China does in the South and East China seas.

- China has spent years building up artificial islands, hoping to cement its claims to waters that Vietnam, the Philippines, Japan, and Taiwan also consider their own.
- Chinese vessels have repeatedly harassed Philippine resupply missions to Second Thomas Shoal, a disputed area off the west coast of the Philippines.²
- The United States has also noted increasing military maneuvers by Chinese jets and ships across all of the disputed waters.³
- Despite China's longstanding claims to territory held by the Philippines, previous Philippine governments have rejected closer military ties with the United States, hoping to maintain a positive trading relationship with China.
- However, the Philippines has established closer U.S. ties since the election of Ferdinand Marcos Jr. in 2022; Marcos started negotiations on reopening four U.S. military bases.⁴
- China's initial response to these closer ties was stepped-up military aggression against the Philippines.⁵

China's relationships with almost all its neighbors have been strained in recent years as those countries have developed closer ties to the United States. This makes China's neighbors likely candidates to be targeted by Chinese-supported cyber threat actors.

- For decades, many traditional U.S. allies (like Australia, New Zealand, and the Philippines) have sought closer relations with China and have seemingly tried to balance the security threat of doing so with the economic opportunities offered by preferential trade access with China.

2

[hXXps://maritime-executive\[.\]com/article/philippines-budgets-for-a-permanent-structure-at-second-thomas-shoal](https://maritime-executive.com/article/philippines-budgets-for-a-permanent-structure-at-second-thomas-shoal)

3

[hXXps://www.theguardian\[.\]com/us-news/2023/oct/18/us-accuses-china-of-pattern-of-dangerous-air-force-manoeuvres-against-military-planes](https://www.theguardian.com/us-news/2023/oct/18/us-accuses-china-of-pattern-of-dangerous-air-force-manoeuvres-against-military-planes)

4

[hXXps://www.aljazeera\[.\]com/news/2023/4/3/philippines-announces-locations-of-4-bases-to-be-used-by-us-army](https://www.aljazeera.com/news/2023/4/3/philippines-announces-locations-of-4-bases-to-be-used-by-us-army)

⁵ [hXXps://edition.cnn\[.\]com/2023/12/13/asia/china-philippines-maritime-standoff-analysis-intl-hnk-ml/index.html](https://edition.cnn.com/2023/12/13/asia/china-philippines-maritime-standoff-analysis-intl-hnk-ml/index.html)

- However, since the pandemic, the United States has made inroads with China's neighbors, seemingly due to China's use of trade as a weapon, theft of intellectual property, increasing claims to its neighbors' territory, and other non-diplomatic behavior.

All of the strategic nations in the region have grown closer to the United States in recent years, effectively creating an unbroken link from South Korea and Japan all the way to Australia.

- In September 2021, the United States and the United Kingdom (UK) announced the AUKUS partnership to provide Australia with nuclear submarines.⁶
- The primary purpose of the AUKUS partnership and the Five Eyes security and intelligence alliance (comprising the United States, the UK, Australia, New Zealand, and Canada) now is to counter the Chinese presence in the Pacific region.
- Australia and New Zealand have veered closer to the United States since China launched a damaging trade war against Australia for backing the U.S. position on China's culpability for the spread of COVID-19⁷ and after growing Chinese assertiveness in the Pacific region, where China approached numerous smaller islands about establishing military bases and notably achieved a security agreement with the Solomon Islands.⁸

Japan and South Korea have recently mended geopolitical fissures dating back decades to create a powerful trilateral alliance with the United States over a shared distrust of China and North Korea.

- Japan has notably gone further and publicly stated that it would send warships to the Philippines in the event China attacks.⁹
- Japan has also announced it is increasing cooperation with Malaysia on maritime security, hoping to create independent linkages to the South China Sea.¹⁰

⁶ [hXXps://www.bbc\[.\]com/news/world-58564837](https://www.bbc.com/news/world-58564837)

⁷ [hXXps://foreignpolicy\[.\]com/2021/11/09/australia-china-decoupling-trade-sanctions-coronavirus-geopolitics/](https://foreignpolicy.com/2021/11/09/australia-china-decoupling-trade-sanctions-coronavirus-geopolitics/)

⁸ [hXXps://gjia.georgetown\[.\]edu/2022/12/02/china-solomon-islands-security-agreement-and-competition-for-influence-in-oceania/](https://gjia.georgetown.edu/2022/12/02/china-solomon-islands-security-agreement-and-competition-for-influence-in-oceania/)

⁹ [hXXps://www.japantimes\[.\]co\[.\]jp/news/2024/01/16/japan/politics/philippines-japan-security-pact/](https://www.japantimes.co.jp/news/2024/01/16/japan/politics/philippines-japan-security-pact/)

¹⁰ [hXXps://thediplomat\[.\]com/2023/12/japan-malaysia-announce-diplomatic-upgrade-enhanced-security-cooperation/](https://thediplomat.com/2023/12/japan-malaysia-announce-diplomatic-upgrade-enhanced-security-cooperation/)

- China is unlikely to accept a militarily assertive United States and Japan threatening its sea lanes.

This effectively leaves China facing an entire wall of U.S.-backed allies containing its expansion and would enable the United States to blockade China economically and militarily in the event of a war. China's declining influence in the Pacific does not end there; its economic downturn has left China with less to offer its neighbors. As a result, other countries with historic trade ties to China are establishing economic opportunities with the United States.

Vietnam has emerged as a key alternative manufacturing hub for companies that no longer want to operate in China. Japan, Taiwan, and South Korea have agreed to U.S. trade restrictions under the Chips and Science Act, which reduces China's access to advanced semiconductor manufacturing.

Lastly, almost the entirety of the region will join the Indo-Pacific Economic Framework for Prosperity (IPEF) when it goes into effect on February 24, 2024. The IPEF is designed to create alternative supply chains for the rare-earth metals that are increasingly needed in advanced and clean technology and whose processing is dominated by China.¹¹

- The trade deal aims to strengthen supply chains that rely on the Pacific Oceans and includes the United States, Australia, Brunei, Fiji, India, Indonesia, Japan, South Korea, Malaysia, New Zealand, the Philippines, Singapore, Thailand, and Vietnam.¹²
- Scarred by previous bouts of trade retaliation by China, these nations are seeking closer U.S. economic ties.
- On February 8, 2024, ZeroFox identified a data leak by the hacker group Philippines Exodus Security against Manila Freight Forwarders, a Philippines-based shipping company specializing in international trade. The same day, Philippines Exodus Security announced an alliance with another hacker group known to attack entities in the region, Sylhet Gang-5g, which recently targeted South Korean entities over their support for Israel.

¹¹

[hXXps://www.commerce\[.\]gov/news/press-releases/2024/01/us-department-commerce-announces-upcoming-entry-force-ipef-supply-chain](https://www.commerce.gov/news/press-releases/2024/01/us-department-commerce-announces-upcoming-entry-force-ipef-supply-chain)

¹²

[hXXps://ustr\[.\]gov/trade-agreements/agreements-under-negotiation/indo-pacific-economic-framework-prosperity-ipef](https://ustr.gov/trade-agreements/agreements-under-negotiation/indo-pacific-economic-framework-prosperity-ipef)

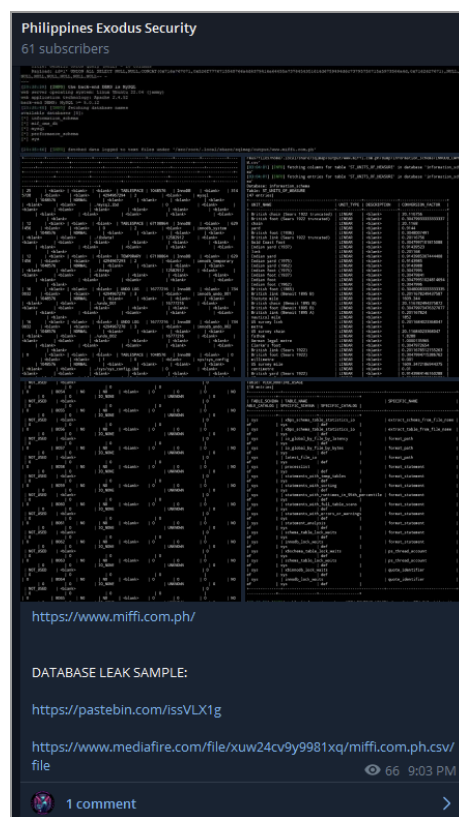


Image of Manila Freight Forwarders data leak posted by Philippines Exodus Security

Source: ZeroFox Intelligence



Image Showing Philippines Exodus Security is collaborating with Sykhhet Gang SgOfficial

Source: ZeroFox Intelligence

Conclusion

Not only do U.S. efforts to isolate China appear to be working, but China's neighbors appear to be creating military and economic alliances that isolate China.

The United States is clearly better-positioned than China currently vis-à-vis the Pacific region due to having:

- Established trilateral ties with Japan and South Korea, despite the politics;
- Established the AUKUS initiative;
- Grown its military and economic ties with Vietnam and the Philippines; and
- Ushered in the IPEF, which is about to go into force.

As China's list of allies in the region shrinks—yet its ambitions to control the seas in the region remain—it will need to find alternative means to project power.

- China has historically used a mix of policy responses to pressure its neighbors.
- In Taiwan, China used economic, military, and cyber threats to influence the recent Taiwanese elections. Nevertheless, its preferred candidate finished second.
- China has threatened its neighbors with trade retaliation and has made efforts to sow distrust in the local population against the United States.

China's own economy is too weak to escalate tensions with the United States and its allies at the moment, although there could be a return to this sort of activity if the Chinese economy sufficiently recovers. China will still likely engage in aggressive military incursions against its neighbors, but these efforts are unlikely to escalate or be intended to start a wider conflict. Rather, China likely feels the need to demonstrate its superior military capabilities to its neighbors regularly.

However, China is likely to escalate its cyber activities against U.S.-allied states in the region. China has an acute need for data and information on the military and economic plans of its allies, and there will likely be an increase in cyber espionage by Chinese threat actors against both private and public organizations—especially those involved in technology manufacturing and international trade in areas in which China also specializes.

- Entities tangentially linked to these industries—such as academic researchers or different parts of the supply chain—will also very likely continue to be targeted.
- Attacks are likely to range from espionage and intellectual property theft to sabotage via the deployment of data-wiping malware, as seen in the Russia-Ukraine war.¹³

¹³ [hXXps://www.wired\[.\]com/story/ukraine-russia-wiper-malware/](https://www.wired.com/story/ukraine-russia-wiper-malware/)

Appendix A: Traffic Light Protocol for Information Dissemination

	Red	Amber
WHEN SHOULD IT BE USED?	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	Sources may use TLP:AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.
HOW MAY IT BE SHARED?	Recipients may NOT share TLP:RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.	Recipients may ONLY share TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. Note that TLP:AMBER+STRICT restricts sharing to the organization only.
	Green	Clear
WHEN SHOULD IT BE USED?	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.	Sources may use TLP:CLEAR when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.
HOW MAY IT BE SHARED?	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels.	Recipients may share TLP:CLEAR information without restriction, subject to copyright controls.

Appendix B: ZeroFox Intelligence Probability Scale

All ZeroFox intelligence products leverage probabilistic assessment language in analytic judgments. Qualitative statements used in these judgments refer to associated probability ranges, which state the likelihood of occurrence of an event or development. Ranges are used to avoid a false impression of accuracy. This scale is a standard that aligns with how readers should interpret such terms.

Almost No Chance	Very Unlikely	Unlikely	Roughly Even Chance	Likely	Very Likely	Almost Certain
1-5%	5-20%	20-45%	45-55%	55-80%	80-95%	95-99%