Police Say To Carry This
Police say everyone should carry this new safety d
that protects against attackers.
OPEN

# The Cyber Dimension of the South China Sea Clashes

China's alleged cyberattacks come amid rising sentiments in the Philippines over the South China Sea disputes.

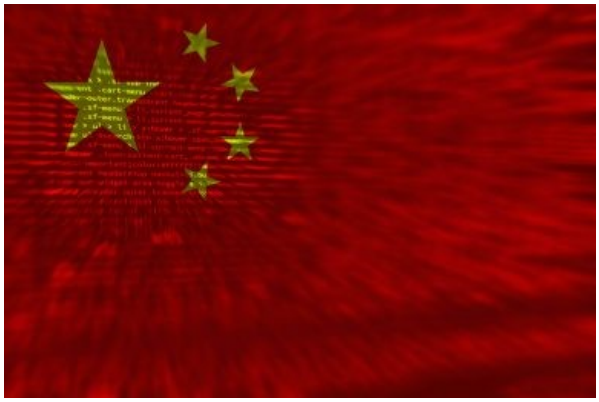

Image Credit: Illustration by Catherine Putz

By Mark Manantan
August 05, 2019

Three years since the Philippines won its landmark victory at the Permanent Court of Arbitration (PCA) at The Hague against China's overlapping claims in the West Philippine Sea or the South China Sea, the majority of Filipinos still demand that the Duterte government enforce the arbitral ruling. In a recent survey, 87 percent of Filipinos want the Duterte government to "arrest and prosecute" Chinese fishermen for destroying marine life in Philippine waters, especially in light of the recent "maritime collision" involving 22 Filipino fisherman and a Chinese vessel in Reed Bank.

However, whenever a sizeable plurality of Filipinos pressures their commander-in-chief to stand up against China, President Rodrigo Duterte reduces the policy options available into a binary choice between war or appeasement. Such an approach seeks to perpetuate a superficial narrative that, in the long run, generates a psychological belief in a false and narrow path to resolving the issue. Halfway through his presidency, the overarching formula to Duterte's approach to China is the oversimplification of geopolitical tensions on the ground, often devoid of facts, which consequently distorts a complex reality. Abetted by his overt theatrics, Duterte conditions his supporters and the public to play by China's rules to avoid any military confrontation, which the Philippines cannot win anyway.

But China's approach toward the South China Sea has never relied on one-dimensional or oversimplified tactics. Instead, it draws from a highly sophisticated political, economic, and strategic arsenal. War or military confrontation remains on the table, but closer examination reveals that — contrary to Duterte's all-or-nothing calculation — China has continuously utilized evolving approaches to cement its unilateral control of the resource-rich stretch waters. That nuanced approach includes cyberattacks.

**Enjoying this article?** Click here to subscribe for full access. Just $5 a month.

A report recently published by enSilo found that the Chinese cyber espionage group called the Advanced Persistent Threat group 10 or APT10 deployed two malicious software variants that targeted government and private organizations in the Philippines in April. According to enSilo's investigation of the malware, the tactics, techniques, procedures, and codes perpetuated by the threat actor are all unique to APT10. In the same month, the Philippine-based Analytics Association of the Philippines (AAP) detected Chinese-related scripts that were inserted in the source code of various government websites such as malacanang.gov.ph, dict.gov.ph, comelec.gov.ph, pnp.gov.ph, navy.mil.ph, and laguna.gov.ph. AAP contends that the implemented scripts were aimed to intercept various systems and to collect information from the target users.

These incidents are not new. China has repeatedly employed cyberattacks linked to the South China Sea issue. The Philippines and China were involved in a mutual cyber conflict during the standoff at Scarborough Shoal and the

Spratly Islands in 2012. However, the re-emergence of suspected Chinese-linked cyberattacks poses an anomaly – one standing in stark contrast to the Duterte government's guarantee regarding China's benign intentions in the cyber realm.

As China's cyberattacks resurface, it is vital to pay particular attention to the political and strategic currency of such malicious activities. The timing and the intent of such cyber operations warrants an interrogation. The recent recorded attacks in April coincided with major developments in the Philippines' security and strategic environment emanating from its internal and external affairs. Both developments are highly interrelated to the South China Sea.

Following reports from the Armed Forces of the Philippines Western Command on the sustained presence and swarming activities of 275 Chinese maritime militia vessels, complemented by the Chinese Coast Guard, in the waters around Philippine-controlled Pag-Asa Island, Duterte issued his most provocative statement to date against China. He pledged to send his soldiers on a suicide mission if Beijing oversteps the "red line." Duterte's comments were a defiant exception to his usual conciliatory approach toward China. Against such a backdrop of heightened tensions with China, the United States and the Philippines renewed their strategic relations, as signified by Duterte's acceptance of U.S. assurances to defend the Philippines if any armed conflict ensues in the South China Sea. The Philippines' resolve was further supported by the U.S. Navy's top admiral, who said the United States would begin classifying Chinese militia vessels as navy warships.

Furthermore, April was also the penultimate month before the finalization of the 20-year negotiation between the Philippines and Indonesia on their maritime boundary treaty based on the 1982 United Nations Convention on the Law of the Sea (UNCLOS). Such an agreement delimits the overlaps in the two archipelagic states' exclusive economic zones (EEZs).

The uptick in Chinese cyberattacks within this period might be a reaction to those recent developments. State-sponsored hackers could be seeking to access valuable information to track if Duterte's rhetoric could translate to actual policies that will push back against China's grey zone tactics, especially with the reinvigorated support from Washington's security commitments to Manila. Obtaining critical communications data for intelligence gathering provides China the leverage to revitalize its current grey zone approach, especially as the Philippines began to explore other innovative strategies to project its control over the islands held by Manila. Meanwhile, the maritime agreement between the Philippines and Indonesia also offers an improved outlook on how other ASEAN member states can peacefully resolve their issues using the arbitral ruling as a key reference, which China vehemently rejects.

The recent cyberattacks are also reminiscent of Chinese cyber espionage activities under the "NanHaisHu" or South China Sea Remote Access Trojan program in August 2016, where hackers extracted confidential information from the Philippines' Department of Justice and the major international law firm that represented nation-states at the PCA at the Hague. Related attacks also concurred during the height of the Philippines' landmark victory in July 2016. The resurgence and potential persistence of Chinese-state sponsored hackers such as APT10 in 2019 raises yet again the question of China's hand in critical infrastructures. Despite assurances from the Duterte government, the current incident revives the argument that China could potentially leverage its 5G technology and wireless systems for intelligence-gathering overseas to exert influence within the target country's domestic politics as well as in the broader international political terrain.

China's cyberattack could also be a pre-emptive strategy in the ongoing discussion of ASEAN's Single Draft of the Code of Conduct (COC), which is expected to be completed in 2019. As the lead coordinator of the COC, the Philippines has expressed the urgent need to fast track its completion in light of the recent maritime collision. Such developments will shape the mechanisms embedded in the COC to deter or confront Chinese evolving aggression, thus opening the possibility for new modifications.

China has a track record of conducting cyberattacks to obtain an advantage in negotiating its demands. Based on a report published by FireEye, Chinese sponsored hackers have consistently targeted Southeast Asian government and military organizations using spear-phishing emails to obtain intelligence information relating to the maritime disputes. Through infiltration, China gains an unfair advantage through access to critical information regarding strategic national interests ahead of negotiations. China could employ a similar strategy to spin the ongoing COC talks to its benefit by devising other counternarrative tactics such as spreading fake news, disinformation, or even compromising the personal information of Southeast Asian diplomats involved in the matter.

It remains unclear if the recent activity of Chinese hackers will be short-lived or part of an entirely new coordinated plan to enforce China's *de facto* control of the area. Attribution remains a fundamental challenge in identifying specific perpetrators; it is especially difficult to determine if such attacks were directed by China's state-sponsored hacking group or the work of patriotic "hacktivists." Nevertheless, existing and growing historical evidence garnered from the forensics of codes and procedures that are unique to Chinese hackers like APT10 indicate that the motivation behind past and present cyberattacks remain consistent — to obtain vital information that is instrumental for China's political, diplomatic, and strategic maneuvering or (in a worst-case scenario) in launching cyberwarfare to paralyze critical infrastructure. The point is, the use of cyberattacks will remain to be a significant tool in advancing Chinese interests in the South China Sea.

The Duterte government is once again advised to rethink its China strategy in the South China Sea. Manila must craft a coherent and a more nuanced approach in the face of evolving Chinese aggression without undermining the "renewed" ties of Sino-Philippines relations — a strategy that Duterte often overlooks in favor of his typical theatrics and penchant for attention-grabbing headlines and antics. Perhaps revisiting the arbitral ruling as Duterte approaches his final three years in office could be a good starting point.

*Mark Manantan is a research fellow at the Center for Southeast Asian Studies at the National Chengchi University in Taiwan, and a research affiliate of Manila-based think tank, Asia Pacific Pathways to Progress. He is the founder of Bryman media. Views expressed are entirely personal.*

**You have reached the limit** of 5 free articles a month. You have read **2** of your **5 free articles** this month.

**Subscribe** to
**Diplomat All-Access**

Enjoy **full access** to the website *and* get an automatic subscription to our magazine with a *Diplomat All-Access* subscription.

**SUBSCRIBE NOW**

Already a subscriber? **Login here**