age Credit: Chinese internet bar image via pcruciatti
hutterstock.com

The Chinese Cyber Threat in the South China Sea

ASEAN needs to get serious about the role of cyberspace in conflicts over the South China Sea.

By Anni Piiparinen
September 18, 2015

As China expands its foothold in the Spratly islands, piling sand and building airstrips on the contested reefs in the middle of the South China Sea, the world has turned its attention back to the territorial disputes that have lingered in the region for decades. While naval strategies and broader military doctrine have dominated the recent headlines, one crucial element of modern conflict has been surprisingly missing from the debate over the South China Sea: cyberspace.

If the past is any guide, however, future escalation in the disputed waters is likely to spill over to the cyber realm regardless of where it starts. According to reports by FireEye, Kaspersky Lab's Securelist, and CrowdStrike, the Southeast Asian claimants to the South China Sea, along with private companies doing business in the region, have been popular targets of advanced intrusion operations originating from China. Chinese cyber units and malware variants have successfully infiltrated public networks in the region, primarily targeting top-level government agencies and civil and military organizations in the Philippines and Vietnam.

China's activities in cyberspace are a means to achieve its goals in the physical world and carry serious potential for escalating lingering tensions into a full-on battle, both on- and offline. Beijing has used its cyber capabilities to accompany other, often diplomatically risky, moves. Indeed, the volume of cyberattacks has significantly increased at times of heightened tensions, with China seeking to gather sensitive security details to gain a strategic edge over its regional rivals.

For example in May 2014, China dragged an oil rig into waters claimed by Vietnam, sparking an international incident. Vessels from both countries engaged in water-cannon battles and deadly anti-China protests erupted in Vietnam. China took the conflict from land and sea to cyberspace, targeting Vietnamese government and military agencies via spear-phishing campaigns that spread documents containing malware. The threat actors likely succeeded in compromising a network belonging to a Vietnamese intelligence agency, gaining access to sensitive information about the country's security strategy.

A notable uptick in China-based cyberattacks against Vietnamese networks also occurred in October 2014, possibly in response to Vietnamese arms acquisitions meant to boost its maritime security capabilities. These incidents

pushed Vietnam to become the most targeted country in cyberspace in 2014, surpassing even the United States.

Vietnam hasn't been the only South Chin Sea claimant targeted by Chinese cyberattacks. In April 2012, Chinese patrol vessels docked in waters near the Philippine-claimed Scarborough Shoal. After a tense standoff, the Philippines was forced to withdraw its ships. At the same time, hackers from both sides launched extensive defacement campaigns of government, media, and university websites. A Chinese cyber unit succeeded in infiltrating Philippine government and military networks, stealing military documents, internal communications, and other sensitive materials related to the dispute.

With the Chinese island-building spree intensifying and the preliminary decision of the arbitral tribunal in the Philippines' legal challenge against China expected by the end of the year, the tensions in the South China Sea will continue to run high. And as the past disputes in the region clearly show, conflicts in the physical world will undoubtedly also play out in cyberspace.

Strong cyber defenses are crucial for a nation's ability to protect sensitive national security information and ensure the operability of many of its core functions. However, the cyber capabilities of Vietnam and the Philippines, along with other Association of Southeast Asian Nations (ASEAN) members bordering the South China Sea, range from weak to nonexistent.

Should the tensions escalate into an active conflict and move from cyber espionage and relatively harmless website defacements into causing real damage to critical infrastructure or government networks, the countries of ASEAN would have practically no way of stopping the attacks. And although the United States is geographically far removed from the territorial disputes, its regional alliances – particularly its mutual defense treaty with the Philippines, reaffirmed in 2014 – and its broader strategic interests in the Asia-Pacific would inevitably drag the U.S. into the dispute.

It is therefore past time to start taking the cyber threat in the South China Sea seriously. The Philippines and Vietnam, along with other targeted countries, should direct increasing resources to developing more sophisticated cyber defense architectures to protect military systems and other sensitive networks. This should include providing sufficient funding for national Computer Emergency Response Teams (CERTs) and creating units under the armed forces to centralize the command of cyberspace operations, similar to the U.S. Cyber Command.

On a regional level, ASEAN needs to fast-track its dormant efforts to create a more resilient cybersecurity regime to mitigate the Chinese cyber threat against its members. The organization should take concrete steps to create a permanent coordinating and information-sharing mechanism, either under the ASEAN secretariat or as a stand-alone ASEAN-CERT under the umbrella of the Asia-Pacific CERT. And while the ASEAN Defense Ministers' Meeting does not yet address cybersecurity as a separate topic, it would be a natural forum to better coordinate regional military efforts.

Additionally, the ASEAN Regional Forum (ARF), which the Chinese also participate in, would serve as a suitable venue for establishing regional codes of conduct and confidence building measures for cyberspace, furthering transparency and complementing the ASEAN-only efforts. ARF should work towards a concrete framework for dealing with cyber conflict, similar to its efforts to enhance maritime security, and establish a communications network that could be activated during cyber crises.

The United States, echoing the sentiment of the recently released U.S. Department of Defense Asia-Pacific Maritime Security Strategy, should make it a priority to enhance the cybersecurity capabilities of its regional allies and partners, "both to respond to threats within their own territories as well as to provide [security] more broadly across the region." This can occur through provision of tools, technologies, and training, joint cyber incident response exercises, or information sharing initiatives.

Boosting the region's cyber defenses proactively, before the next major crisis flares up, offers a viable model for regional cooperation aimed at gradually making Southeast Asian militaries more capable, credible, and independent in the cyber realm. It will allow the countries to increasingly take the lead in protecting their territories and networks while letting the United States slowly move to the back seat.

Anni Piiparinen is a program assistant with the Cyber Statecraft Initiative of the Atlantic Council's Brent Scowcroft Center on International Security.