

The rash of defaced foreign websites allegedly carried out by local hacker groups is neither sanctioned nor condoned by the Philippine Government, and must be stopped at the soonest. This is the statement issued by officials from the Department of Science and Technology's Information and Communications Technology Office (DOST-ICTO).

"We understand the concern of our local hacker community on this issue. However, exchanges such as this one will not benefit anyone and could possibly lead to bigger problems in the future for the Philippines and China and escalate the already tense situation at Panatag Shoal," explained Louis Casambre, Executive Director of DOST-ICTO.

Attempts at distributed denial of service (DDOS) from foreign origins on the gov.ph domain were detected recently and promptly blocked by government IT administrators. As a result, access to several government websites were blocked or deliberately delayed arising from the DDOS attacks.

What sparked this series of online vandalism was the defacement of the University of the Philippines website by hackers sympathetic to China's claims on what is known internationally as Scarborough Shoal, a triangle-shaped chain of reefs and islands 220 kilometers off Palauig, Zambales known for the richness of its fishing grounds of its surrounding areas. This sparked a series of retaliations committed by rival hacker groups promoting the cause of Philippine sovereignty on the disputed area against a number of China-based websites.

DOST Secretary Mario Montejo expressed his displeasure on the hacker attacks. "These skirmishes in cyberspace are unsanctioned by either government and are largely outbursts of public sentiment by private citizens from either country regarding the current situation. It is our job in government to seek diplomatic solutions to these issues and not let them get out of hand," Montejo said.

IT experts concur that the hacking of the UP website exposed the vulnerability of certain government sites, prompting renewed calls for tighter, more stringent online security standards.

Casambre noted that along with the cybercrime bill currently undergoing legislative review at both chambers of Congress, the DOST-ICTO is working closely with the Office of the President in drafting an Executive Order to establish a top-level body to spearhead government's efforts on cybercrime and cybersecurity.

"The creation of this body will strengthen the necessary coordination and implementation of uniform security standards in government," he added.