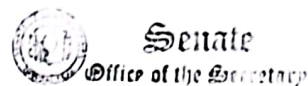



NINETEENTH CONGRESS OF THE)
REPUBLIC OF THE PHILIPPINES)
Second Regular Session)



24 FEB -5 P2 :29

SENATE

P.S.R. No. 923

RECEIVED BY: 

INTRODUCED BY SENATOR RISA HONTIVEROS

RESOLUTION

CALLING FOR THE SENATE COMMITTEE ON NATIONAL DEFENSE AND SECURITY TO CONDUCT AN INVESTIGATION IN AID OF LEGISLATION INTO A FOREIGN GOVERNMENT-SPONSORED CYBER INTRUSION AFFECTING GOVERNMENT AGENCIES, INCLUDING THOSE DIRECTLY INVOLVED IN SAFEGUARDING NATIONAL INTERESTS IN THE WEST PHILIPPINE SEA

WHEREAS, on February 3, 2024, the Department of Information & Communications Technology ("DICT") announced that hackers believed to be operating from within the People's Republic of China ("PRC"), and possibly sponsored or supported by its Chinese Communist Party-led Government, breached the email systems and internal websites of several government agencies including those maintained and operated by the Philippine Coast Guard, the Office of the Cabinet Secretary, the Department of Justice ("DOJ"), the National Coast Watch System ("NCWS"), the House of Representatives, and that of the DICT itself;

WHEREAS, the DICT also reported that several private domains were also targeted, including the personal website of President Ferdinand "Bongbong" Marcos, Jr.;

WHEREAS, the cyberattack – which was described by the DICT as "academically perfect," was reportedly carried by one of the three Chinese state-sponsored cyber-intrusion groups classified as Advanced Persistent Threats ("APTs"): Lonely Island, Meander, and Panda;

WHEREAS, in a Joint Cybersecurity Advisory ("CSA") recently issued by the United States' National Security Agency ("NSA"), Cybersecurity and Infrastructure Security Agency ("CISA"), and Federal Bureau of Investigation ("FBI"), it was reported that PRC state-sponsored cyber activities continue to target government and critical infrastructure networks with an increasing array of new and adaptive techniques – some of which pose significant risks to defense sector networks;

WHEREAS, late last year, according to Unit 42, a Palo Alto research arm closely studying cyber-attacks, a series of attacks targeting a Southeast Asian government was found to have been carried out by three separate threat actors affiliated with Chinese interests, in which multiple critical government entities were compromised;

WHEREAS, after the cyber-intrusion, the state actors attempted to install other tools and malware to maintain a foothold in the environment and establish persistence, for the purpose of long-term surveillance;

WHEREAS, recently, the PCG has been tasked with escorting resupply missions to the B.R.P. Sierra Madre, which missions have been invariably unlawfully harassed, obstructed, and impeded by vessels belonging to the China Coast Guard and so-called Chinese maritime militia; and

WHEREAS, considering the possibility that malware has been installed on Philippine critical defense networks for the purpose of long-term surveillance, these recent cyber-intrusions threaten to compromise resupply missions to Ayungin shoal, the security of Philippine Armed Forces personnel stationed on the B.R.P. Sierra Madre, and wider Philippine national interests in the West Philippine Sea.

NOW THEREFORE, BE IT RESOLVED AS IT IS HEREBY RESOLVED TO CALL FOR THE SENATE COMMITTEE ON NATIONAL DEFENSE AND SECURITY TO CONDUCT AN INVESTIGATION IN AID OF LEGISLATION INTO A FOREIGN GOVERNMENT-SPONSORED CYBER INTRUSION AFFECTING GOVERNMENT AGENCIES, INCLUDING THOSE DIRECTLY INVOLVED IN SAFEGUARDING NATIONAL INTERESTS IN THE WEST PHILIPPINE SEA.

Adopted.


RISA HONTIVEROS
Senator