



SEVENTEENTH CONGRESS OF THE)
REPUBLIC OF THE PHILIPPINES)
First Regular Session)

'17 MAY 17 P2:04

RECEIVED BY: _____

SENATE

P.S. Resolution No. 381

Introduced by: Senator Paolo Benigno "Bam" A. Aquino IV

A RESOLUTION DIRECTING THE APPROPRIATE SENATE COMMITTEES TO CONDUCT AN INQUIRY, IN AID OF LEGISLATION, ON THE RECENT GLOBAL RANSOMWARE CYBERATTACKS AND THE IMPLEMENTATION OF THE NATIONAL CYBERSECURITY PLAN 2022 WITH THE END VIEW OF PROTECTING THE FILIPINO PEOPLE, INSTITUTIONS, AND INFORMATION RESOURCES FROM CYBERATTACKS AND OTHER CYBER THREATS

WHEREAS, in accordance with Republic Act No. 10844, otherwise known as the "Department of Information And Communications Technology Act of 2015," the DICT is mandated to "ensure and protect the rights and welfare of consumers and business users to privacy, security and confidentiality in matters relating to ICT, in coordination with agencies concerned, the private sector and relevant international bodies;"

WHEREAS, under Republic Act No. 10844, the DICT is assigned all powers and functions related to cybersecurity, including but not limited to the formulation of the National Cybersecurity Plan and the facilitation of international cooperation on intelligence regarding cybersecurity matters;

WHEREAS, the DICT unveiled the National CyberSecurity Plan 2022 last May 2, 2017. This Plan seeks to: (1) assuring the continuous operation of our nation's critical information infrastructures, public and military networks (2) implementing cyber resiliency measures to enhance our ability to respond to threats before, during and after attacks, (3) effective coordination with law enforcement agencies and (4) a cybersecurity educated society;¹

WHEREAS, the National CyberSecurity Plan 2022 aims to institutionalize the adoption of Information Security Governance and Risk Management approaches that are based on global standards. Moreover, it seeks to establish the National Computer Emergency Response Team (NCERT) to enable the government to swiftly respond and recover from cyberattacks;

WHEREAS, last 12 May 2017, a massive cyberattack hit at least 150

¹ <http://www.dict.gov.ph/national-cybersecurity-plan-2022/>

countries and infected 300,000 machines. Victims include hospitals, universities, businesses and government agencies;

WHEREAS, according to news reports, a malicious software called 'ransomware' infiltrated computers around the world, from the delivery giant FedEx in the United States to Britain's public health system, reaching universities in China and even Russia's powerful Interior Ministry;²

WHEREAS, ransomware is a program that gets into a computer, either by clicking on an infected link or downloading an infected file, and locks and encrypts the computer files for ransom. If unpaid, the ransom increases over time until the end of a countdown, when all the files are destroyed;

WHEREAS, this attack used the program known as *WanaCrypt0r 2.0* or *WannaCry*, that exploits a vulnerability in the Windows Operating System. Experts say that *WannaCry* is not just a ransomware program, it is also a worm that infects a computer and looks for other computers to spread itself;³

WHEREAS, aside from its detrimental and costly impact on work operations, cyberattacks can also endanger lives as demonstrated in the recent *WannaCry* attack on the National Health Service (NHS) of Britain, where emergency rooms, doctor's offices and ambulances were disrupted, all at the expense of the patients;

WHEREAS, the National Bureau of Investigation (NBI) has not received any report of a *WannaCry* attack incident so far. Nevertheless, the Secretary of Justice ordered the NBI to address the new threat through monitoring and stepping up of our cyber security measures to prevent or at least minimize the adverse effect of a possible attack;⁴

WHEREAS, Supt. Jay Guillermo, spokesman for the PNP's Anti-Cybercrime Group (ACG), asserted that there must be continuous coordination and collaboration among private institutions, government and law enforcement agencies for investigation and cyber response. The PNP further noted that internet service providers should help authorities look into the cyberattack;⁵

WHEREAS, experts have advised computer users to exercise caution in opening emails and links. They further advise users to regularly back up their data and promptly install the latest security updates on their gadgets as soon as these become available;⁶

²<https://www.nytimes.com/2017/05/12/world/europe/international-cyberattack-ransomware.html>

³<https://www.theguardian.com/technology/2017/may/12/global-cyber-attack-ransomware-nsa-uk-nhs>

⁴<http://www.philstar.com/headlines/2017/05/15/1700077/government-steps-cybersecurity-amid-wannacry>


⁵<http://www.philstar.com/headlines/2017/05/15/1700077/government-steps-cybersecurity-amid-wannacry>

⁶ <http://www.philstar.com/world/2017/05/13/1699589/explainer-what-ransomware>

WHEREAS, the DICT is monitoring the reported ransomware attack in various countries. Assistant Secretary and Cybersecurity Group head Allan Cabanlong stated that the cyberattack highlights the need for the Philippine government to step up its cybersecurity measures;⁷

NOW, THEREFORE, BE IT RESOLVED, as it hereby resolved by the Senate of the Philippines to direct the appropriate Senate committee to conduct an inquiry, in aid of legislation, on the recent global ransomware cyberattacks and the implementation of the National Cybersecurity Plan 2022 with the end view of protecting the Filipino people, institutions, and information resources from cyberattacks and other cyber threats.

Adopted,

A handwritten signature in black ink, appearing to read "Bam Aquino". The signature is written in a cursive, flowing style.

⁷ <http://www.philstar.com/headlines/2017/05/15/1700077/government-steps-cybersecurity-amid-wannacry>