GOVERNMENT OF INDIA
MINISTRY OF SHIPPING

LOK SABHA

UNSTARRED QUESTION NO.2029

TO BE ANSWERED ON 27th JULY, 2017

IMPACT OF CYBER ATTACK ON PORT

2029. DR. KAMBHAMPATI HARIBABU:

Will the Minister of SHIPPING be pleased to state:

(a)   whether it is a fact that operations at Jawaharlal Nehru Port, Mumbaiwere
        affected after an incident of cyber-attack recently;
(b)   if so, the details thereof;
(c)   whether the Government proposes to upgrade cyber security at all the ports in
        the country to prevent recurrence of such attacks in future; and
(d)   if so, the details thereof?

ANSWER
MINISTER OF STATE IN THE MINISTRY OF SHIPPING
(SHRI PON. RADHAKRISHNAN)

(a)&(b): Yes, Madam. The Arnold Peter Moller (APM) Maersk Terminal, one of
        the four container terminals operating at Jawaharlal Nehru Port Trust
        (JNPT), reported a Cyber attack on their Terminal Operating System at
        4.30 P.M. on 27.06.2017. This attack hadaffected all the facilities of
        APM Maersk Group in Europe and in India, having the corporate office
        at Copenhagen, Denmark and their central IT infrastructure at The
        Hague. However, the APM Terminal achieved normal performance
        parameters from the evening of 4th July, 2017. The other three
        Container Terminals at JNPT were not impacted by the malware attack
        and continued to function normally.

(c)&(d):Yes, Madam. Major Ports have been advised to coordinate with National
        Cyber Security Coordinator (NCSC) for cyber security audit. NCSC has
        been requested to hold sensitization workshop to help frame
        appropriate draft guidelines with respect to Cyber Security to be
        implemented by the ports. In addition, to prevent Ransomware attacks,
        Ministry of Electronics and Information Technology (MEITY) has also
        taken the following steps:
(i)   CERT-In has issued an advisory regarding detection and prevention of
        PetyaRansomware on its website on 27th June, 2017.
(ii)   CERT-In has issued a vulnerability note on its website suggesting
        information regarding vulnerabilities in Microsoft Windows Systems
        which have been exploited by PetyaRansomwarealongwith remedial
        measures.
(iii)   Free tools for detection and removal of bots including
        PetyaRansomware have been provided on the website of Cyber
        Swachhta Kendra (www.cyberswachhtakendra.gov.in).
                              *****