

**DEPARTMENT: PUBLIC ENTERPRISES**

**REPUBLIC OF SOUTH AFRICA**

**NATIONAL ASSEMBLY**

**QUESTION FOR WRITTEN REPLY**

**QUESTION NO.: 1893**

**QUESTION:**

**1893. Mr G K Y Cachalia (DA) to ask the Minister of Public Enterprises:**

In light of the fact that Transnet Port Terminals (TPT), the state-owned freight company’s division that operates the container terminals at the biggest ports of the Republic, including Cape Town, Port Elizabeth, Ngqura and Durban, has declared force majeure late on 26 July 2021 after its IT systems suffered a massive cyberattack the previous week that crippled its operations, (a) what is the extent and effect of the attack, (b) what is being done to (i) mitigate effects of the attack and (ii) ensure no repeat of the attack, (c) how did the attack come about, (d) who was responsible, (e) on what date is it envisaged that TPT operations will return to normalcy and (f)(i) what are the details of the impact of the attack on exports and imports and (ii) how are customers being assisted in the interim?

**REPLY:**

**According to the information from Transnet response:**

(a) Initially all ICT systems were shut down to stop the spread of the malware.  Some servers and some workstations that were online at the time of the attack were encrypted by the ransomware.

(b)(i) An incident response team was brought in to assist with the secure rebuild of the active directory servers. A second incident response team assisted with containing the incident and performing a forensic scan of all machines.

(b)(ii) Transnet was already in the process of rolling out additional security measures across the network. This has been fast-tracked and all machines that are brought back on on-line have the security stack deployed. A separate Endpoint Detection and Response (EDR) and forensic agent has been deployed on all machines before they were brought back online.

All older operating systems have been upgraded to current operating systems and were fully patched before being brought back online.

Transnet has also deployed a web access firewall, reverse proxy and an anti-distributed denial of service system for all public websites.

(c) It was a ransomware attack. There is a criminal investigation in progress.

(d) There is a criminal investigation in progress.

(e) All customer interfaces and the NAVIS terminal operating system have returned to normal. TPT has continued to keep customers and stakeholders informed of the progress made since Thursday 22 July 2021. Transnet will continue to engage in the dedicated daily recovery fora and meetings until all operations and the entire supply chains have normalised. For example, Transnet has a dedicated weekly recovery session with Business Unity South Africa, which commenced on 28 July 2021 and is planned to conclude on 20 September 2021. Other meetings with port stakeholders will continue daily, until congestion has been resolved.

(f)(i)Container volumes were delayed as a result of the cyber-attack or the resulting congestion. However, most imports and exports would still be serviced through SA or neighbouring Ports, albeit later than originally planned.

Automotive vessels were delayed due to system unavailability, which was mitigated by the implementation of manual processes. Some vessels have been diverted between terminals and other delayed volumes have caught up. Hence, the impact on volumes through SA ports is negligible.

In respect of Bulk and Breakbulk cargo, Business Continuity (manual processes) significantly mitigated the potential loss of volumes. No material impact is expected on Bulk and Breakbulk volumes as a result of the system down time.

(f)(ii) TPT will continue to engage in dedicated recovery forums, until all operations and the entire supply chains have normalised.

In addition to the broader fora, TPT engages directly with the shipping lines, to plan jointly to ensure fluid operations at the terminals and on the waterside.