USDA United States Department of Agriculture
Foreign Agricultural Service

GAIN Global Agricultural Information Network

Voluntary Report – Voluntary - Public Distribution **Date:** August 11, 2021

Report Number: SF2021-0048

Report Name: Cyber-Attack Cripples Operations at the Port of Durban for the Second Time in a Month

Country: South Africa - Republic of

Post: Pretoria

Report Category: Agricultural Situation, Agriculture in the News, Citrus, Avocado, Fresh Deciduous Fruit, Fresh Fruit, Grain and Feed, Livestock and Products, Oilseeds and Products, Poultry and Products, Sugar, Tree Nuts, Wine, Avocado, Fresh Deciduous Fruit, Fresh Fruit, Grain and Feed, Livestock and Products, Agricultural Situation, Agriculture in the News, Citrus, Oilseeds and Products, Poultry and Products, Sugar, Tree Nuts, Wine

Prepared By: Makoma Makhopa, Wellington Sikuka, Dirk Esterhuizen, and Katherine Woody

Approved By: Ali Abdi

Report Highlights:

Days after the Port of Durban resumed operations after a period of civil unrest brought the terminal to a standstill, South Africa's state-owned port, rail, and pipeline authority, Transnet, announced that a cyber-attack had again crippled the flow of goods in and out of the country. Transnet was forced to declare force majeure for the second time in a month after the cyber-attack on July 22, which forced port workers to manually track ship movements and resort to a paper-based clearance process for cargo at the Ports of Durban, Cape Town, Ngqura, and Gqeberha. The Port of Durban is the largest port terminal in sub-Saharan Africa, and 60 percent of Southern Africa's containerized trade passes through the harbor. As a result of the cyber-attack, the processing time for imported cargo slowed dramatically as workers were only able to process about three containers per hour, according to Post's contacts.

Situation Overview

Days after the Port of Durban resumed operations after a period of civil unrest brought the terminal to a standstill, South Africa's state-owned port, rail, and pipeline authority, Transnet, announced that a cyber-attack had again crippled the flow of goods in and out of the country. Transnet was forced to declare force majeure for the second time in a month after the cyber-attack on July 22, which forced port workers to manually track ship movements and resort to a paper-based clearance process for cargo at the Ports of Durban, Cape Town, Ngqura, and Geerah. The Port of Durban is the largest port terminal in sub-Saharan Africa, and 60 percent of Southern Africa's containerized trade passes through the harbor. As a result of the cyber-attack, the processing time for imported cargo slowed dramatically as workers were only able to process about three containers per hour, according to Post's contacts.

Systems at the Port of Durban were back online by the evening of July 29, though the other ports were forced to manually process cargo for few more days. Due to a large build-up in containerized cargo, more than a week later the Port of Durban still has a substantial backlog. Refrigerated container cargo was most affected, as the ports ran low on space to store backlogged cold chain cargo. The effects of the cyber-attack added to the difficulties faced by importers of chilled and frozen products after the loss of 40,000 tons of cold storage capacity in the wake of the riots in mid-July. Four major cold chain facilities were forced offline after looting and arson damaged cold chain capacity in the Durban area, according to Post contacts. Only one facility of the four was fully back online as of early August.

Although the cyber-attack mostly affected container terminals, bulk vessels carrying grains were also impacted due to delays at the ports as Transnet started to process shipments manually. Wheat, rice, and corn were among the affected commodities. Some bulk and container vessels also decided to bypass South Africa rather than wait in long shipping queues. These deliveries could be delayed by a month or more, according to one post contact with multiple containers of U.S. consumer-oriented food products on a ship that decided to bypass South Africa during the cyber-attack slowdown.

Post's contacts in the fresh produce and liquor industry confirmed that the cyber-attack caused shipment delays, noticeable backlogs, and a shortage of containers. Despite some port terminals being privately operated and thus not subject to the cyber-attacks, they seem to have been indirectly affected by the congestion and diversion of some ships away from South African ports. There is still uncertainty in how long it will take to clear the backlogs and when affected ports will return to normal operations. However, most contacts in the fruit sector are anticipating delays of at least 2 to 3 weeks to clear the backlog at the Port of Cape Town.

The sections below describe the effects on specific parts of the trade and agricultural sectors in South Africa.

Poultry and Beef

Supply chains and the transport of poultry and beef products have been severely disrupted, worsening an already difficult situation for the sector after some logistics providers and distribution centers were forced to close in the wake of the civil unrest in mid-July. The storage capacity for frozen poultry and meat products was already limited with the loss of cold chain facilities. Concern has only grown with the backlog caused by the cyber-attack. Post contacts indicated that there was increasing pressure on

importers to free up refrigerated containers needed for citrus exports. Cold chain storage capacity in Durban and the Gauteng province are reportedly near capacity.

Around the time that the Port of Durban came back online, the South African Department of Agriculture, Land Reform, and Rural Development (DALRRD) proposed a plan to speed up clearance of backlogged containers by using visual inspections as much as possible and focusing testing on products from exporters with the worst history of violations. DALRRD also instructed inspectors to take samples from released containers as a means of traceability if any other issues arose. They limited transportation of containers to the railway system only, even though most containers typically move by road. As a result, the rail system became extremely congested and the flow of backlogged refrigerated cargo has been slow, according to Post contacts. South African trade associations for the meat industry have appealed to DALRRD to allow cargo to be released for transport via trucks, which typically can move about 50 containers per day from the Port of Durban.

For the domestic poultry industry, the biggest issue is the threat to food security developing as the central distribution centers remain closed and are not accepting product deliveries. The South African Poultry Association estimates that the sector slaughters about 5 million birds a day nationally, with about 30 percent coming from the province of KwaZulu-Natal, home to the Port of Durban. The industry reports that the lack of cold storage could greatly affect the flow of poultry meat in South Africa.

The ability to move animal feed to poultry farms and other livestock sectors has also been severely disrupted and could lead to a massive animal welfare issue for the industry. Some farms reported being without feed for about three days. Hatcheries supply about four million birds per day nationally but cannot get them to farms. Day-old poultry stock that could not be moved to farms throughout the country for placement had to be euthanized.

Post contacts indicate that they have been unable to export beef due to the Transnet cyber-attack. Almost no containers are moving to the ports while the backlog remains, and just a few are leaving the country by air freight.

Fresh Produce

According to the Fresh Produce Importers Association, while the impact of the cyber-attack at the ports is probably higher on agricultural exports, it has also been felt on the import side. The cyber-attack took place at a very busy time of the year for winter fresh produce imports, including stone fruit and table grapes from the Northern Hemisphere. Some importers have complained about consignments being stuck at ports of entry, resulting in a huge cost impact. In addition, these delays are affecting the supply and quality of imported perishable products.

Deciduous Fruits (Apples and Pears)

While the cyber-attack had an impact on deciduous fruit trade during the period when ports were closed, the Port of Cape Town is returning to a more normal operating capacity. Minimal disruptions were experienced for the pome season, which is now winding down and about to end. Most pack-houses reported having adequate space to store the fruit during the disruption. However, as some vessels

bypassed the ports in Cape Town, it is expected that it may take at least 2 weeks to clear the backlogs and return to normal operations.

Table Grapes

It is too early to foresee any impact to the table grapes sector given that the harvest season is at least 3 months away, leaving a lot of time for shipments to return to normal levels.

Avocados

According to Post's contacts, the cyber-attack resulted in some delays, but the extent of the delays is still uncertain.

Pineapples

The pineapple industry had not shipped any containers since the July 22 cyber-attack, with loading expected to resume in the second week of August at best. The cyber-attack together with the disruptions from civil unrest and closure of the Durban port has impacted export sales.

Citrus

Citrus exports were not as affected by the cyber-attack as containerized cargo, since the commodity is typically loaded on break bulk vessels serviced by private terminals in domestic ports. However, the ripple effects of the cyber-attack have still caused a backlog of fruit across the citrus supply chain, with temporary delays for exports to key markets. The Port of Durban still has considerable congestion, as cold stores and pack-houses filled to capacity. Moreover, hundreds of trucks delivering cargo for export were forced to park around the port precinct, a situation that will take some time to normalize.

Tree Nuts

The macadamia industry was impacted by the disruptions at the ports due to the cyber-attack, making it difficult to export macadamia nuts. However, the situation has improved as systems came back online. Macadamia nuts can be stored for long periods, so the port disruptions are not expected to affect the quality of shipments. According to Post's contacts, the sector is not too concerned at this stage as things seem to be returning to normal levels.

Sugar

The cyber-attack had limited impact on bulk raw sugar operations at the privately operated Durban sugar port terminal.

Wine

It is difficult to quantify the impact of the cyber-attack alone, as the wine industry was already impacted by various other factors, including a lack of containers for shipment, domestic sales prohibitions, and limitations of the glass bottle supply and bottle closures. However, the cyber-attack did cause a delay in

wine exports, which could result in late delivery and lost sales in various markets. The wine industry has indicated that wine exports for July 2021 were lower than previous months by at least 4 to 5 million liters, partly due to the cyber-attack and the other factors listed above. The South African win industry is optimistic that operations will normalize in August.

Attachments:

No Attachments.