Scientia Militaria
2023, VOL. 51, NO. 3, 161-186
DOI: 10.5787/51-3-1430

Vulnerability of South African Commodity Value Chains to Cyber Incidents

Brett van Niekerk
Durban University of Technology

Abstract

A commodity value chain can be considered the ‘route’ from the source (provider) to the destination (client), including the various modes of transportation. This will often include some form of road or rail to a port for export to a destination country. Due to the rise in cybercrime and state-backed cyber operations, these commodity value chains may be disrupted, having a cascading effect down the value chain. Previous research has considered this a form of economic information warfare, and has indicated that state-sponsored cyber operations to disrupt a commodity intentionally will most likely fall below the threshold of a ‘use of force’ or ‘attack’ under international law. Subsequently, two pertinent instances of cyber incidents at ports have occurred: the disruption of a major Iranian port, and a ransomware incident at a major South African freight and logistics state-owned enterprise.

Following the disruption resulting from the ransomware incident affecting South African freight organisations, there is a need to analyse the vulnerabilities of the freight transportation sector further, in particular the ports and associated railways in terms of malicious cyber interference. Expanding previous research, this article provides a specific view of the major commodity value chains in South Africa that are supported by the freight transportation infrastructure, their possible vulnerability to cyber incidents, and the potential implications thereof. In addition, publicly available information on the responses to the ransomware incident will be discussed to gauge national readiness in terms of crisis management of a major disruption to the primary trade mechanisms in the country. The article focuses on identifying single points of failure within the commodity value chain, and employs hypothetical scenarios to illustrate possible ramifications of a major incident. The port of Durban is shown to the most critical single point of failure overall. Recommendations include the introduction of a sector-specific computer security incident response team for the freight transportation sector.

Keywords: commodity value chain, critical infrastructure, cyber incident, cybersecurity, maritime security

Introduction

In July 2021, the South African (SA) national freight and logistics organisation suffered a cyber incident that disrupted operations in the container terminals and resulted in freight delays, and *force majeure* was declared at the ports (Gallagher & Burkhardt, 2021; Ginindza, 2021; Njini & Viljoen, 2021). It was estimated that maritime trade contributes between 80% and 90% of the SA economy (Department of Transport [DoT], 2017); however, statistics by the United Nations Conference on Trade and Development (UNCTAD) (2018) show that, at the time, South Africa was losing its prominence in the region based on the liner shipping connectivity index (LSCI). It is therefore imperative that the South African physical freight distributions network be considered in terms of its vulnerability to disruptive cyber incidents, as further significant disruptions will erode the confidence in South Africa as a transport hub. Related to the ports, the railways transport freight between the ports and the source (for export) or destination (for imports).

Problem statement

Trade is the lifeblood of economies, and the majority of the trade is transported through the maritime sector, interconnected with railways. With the severe disruption of SA ports due to a ransomware incident in 2021, the susceptibility of trade routes to cyber interference was demonstrated. There is therefore a need to identify high-level vulnerabilities within the SA freight transportation infrastructure, which supports the nation's major commodity value chains. The objectives of the current study were to –

- conduct an analysis of the physical transport infrastructure supporting the commodity value chains in order to identify critical single points of failure;
- assess the potential impacts of cyber incidents; and
- provide recommendations to mitigate cyber incidents affecting the commodity value chains.

Research design and methodology

The research adopted a positivist standpoint, i.e. a view that the world can be measured. The study therefore analysed the SA freight logistics based on commodity value chains, i.e. the ports, customs, railways and related infrastructure to transport various commodities between the source and destination within the country. In particular, single points of failure are identified at a high level. In the field of critical infrastructure protection, single points of failure are components of a broader system where there is no redundancy, and any failure of this component will result in a severe disruption across the system (Moore, 2018). The contribution of commodities to the national gross domestic product (GDP) and measurements of the throughput of various components of the freight transportation infrastructure (ports and rail routes) are used to calculate potential single points of failure. Hypothetical scenarios are employed to illustrate potential impacts of cyber incidents on the commodity value chains.

The study was limited to a high-level strategic setting, and consequently did not provide in-depth coverage of specific technologies or technical vulnerabilities. The high-level premises can be generalised to apply the analysis to other nations, even though the focus was on the SA situation.

Layout of the article

The article presents a discussion of the SA freight transportation and commodity value chains next, followed by an overview of cybersecurity for physical transportation and commodity value chains. An assessment for potential disruption of the SA freight and maritime environment due to cyber incidents follows to conclude the article.

South African freight transportation and commodity value chains

Overview of value chains

A value chain can be defined as a "system of interdependent activities, which are connected by linkages" (Porter & Millar, 1985:n.p.). In a freight transportation context, commodity value chains can then be considered to contain, but are not limited to, the following processes that enable the transportation of various commodities between the source and destination within the country or internationally (Loomis, Singh, Kessler & Bellenkens, 2021):

- vessel management and navigation;
- piloting and berthing at the ports;
- loading and offloading cargo from vessels;
- customs processes;
- information technology (IT) systems to manage the port and cargo in the port precinct;
- loading and offloading cargo from trains and trucks;
- access control for trucks;
- switching and control of railways;
- toll booths for major roads; and
- dispatch and receiving processes at the source and destination respectively.

Figure 1 provides a high-level conceptualisation of a hypothetical commodity value chain from the point where the commodity is being dispatched from the source, until the time it is received at the destination.

Freight transportation and commodity value chains in South Africa

In South Africa, there are nine key commodities that contributed 42.9% of the national GDP in the 2020–2021 financial year, namely (in order of contribution): agriculture (~12.5%), containers (~12%), automotive (~7%), liquid fuels (~6%), coal (~3%), iron ore (~1.5%), manganese (~1%), chrome and magnetite (~0.5%) (Transnet, 2021a). Of these, the top four commodities contribute approximately 37% of the GDP.

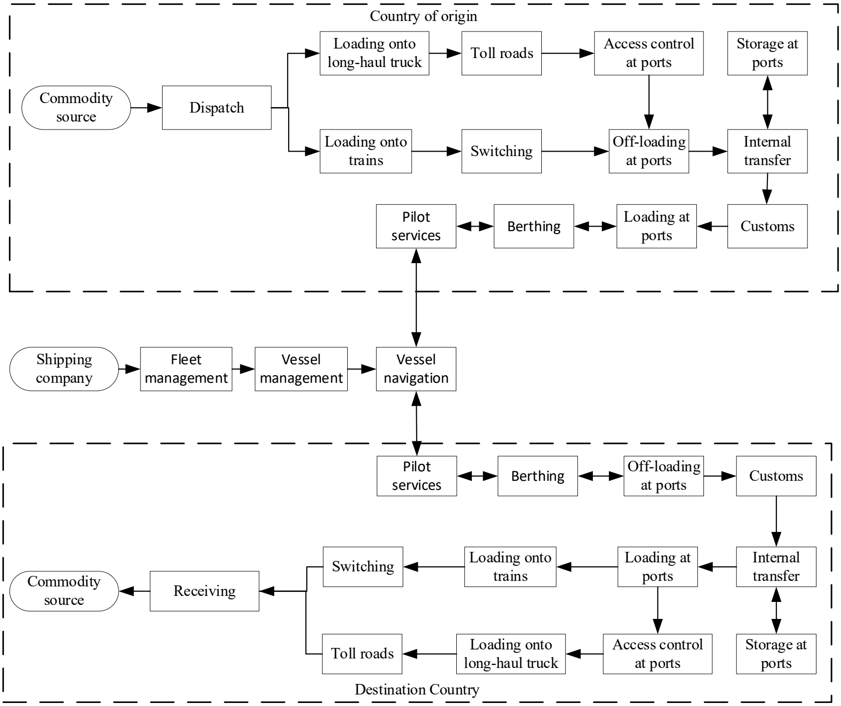

Figure 1: High-level perspective of a value chain

Table 1 below provides an overview of the commodities at and capacities of the SA ports. In addition to the data below, each port has a focus on specific mineral or agricultural products. For mineral bulk, Port Elizabeth handles manganese; Richards Bay deals with numerous mineral products, but primarily coal; and Saldanha handles iron ore and steel products. Wheat and maize are transported through Durban and East London; fresh produce is handled at Cape Town; and Durban handles woodchips, soya bean meal, and animal feed (Transnet Port Terminals [TPT], 2013a).

Table 1: Commodity capacities for South African ports

	Agricultural bulk	Break bulk	Mineral bulk	Automotive	Containers
Cape Town	1.5 mtpa	1.5 mtpa			1.4 TEU
Durban	1.4 mtpa	1.6 mtpa		520 000 FBUs	3.6 TEU
East London	0.76 mtpa	0.21 mtpa		139 000 FBUs	
Ngqura					2.0 TEU
Port Elizabeth			6 mtpa	158 000 FBUs	0.4 TEU

	Agricultural bulk	Break bulk	Mineral bulk	Automotive	Containers
Richards Bay			28 mtpa		
Saldanha		3.0 mtpa	63 mtpa		

Note: mtpa = million tons per annum; FBUs = fully built-up vehicle; TEU = twenty-foot equivalent unit

Source: TPT (2013a)

Key IT systems for the ports include Navis Sparcs N4, General Cargo Operating System (GCOS), and electronic data interchange (EDI). Navis focuses on the container terminals and was first introduced in 2007 before being implemented at other terminals. Navis provides integration with the rail freight since 2012. There is a single instance of Navis for all terminals (TPT, 2013c). The main function of Navis is to keep track of the cargo containers on vessels and in the yards to allow them to be fetched and moved efficiently, and the system can provide some optimisation of routing and stowing (Navis, 2021). GCOS is developed and supported in-house and focuses on multi-purpose terminals and the automotive terminals. EDI is a common standard method of exchanging computer-to-computer information (TPT, 2013b).

While TPT provides cargo-handling services, Transnet National Port Authority (TNPA) provides navigation and port services, including lighthouses and dredging. The berthing infrastructure at SA ports includes 19 berths servicing containers, 36 dry-bulk berths, 29 break-bulk berths, and 13 liquid-bulk berths (Transnet National Ports Authority [TNPA], 2010).

There is approximately 31 000km of rail track, which translates to approximately 21 000km of rail routes across South Africa (Transnet, 2021b). Key links and commodities transported by rail compared to road freight transportation are illustrated in Table 2. As is evident, other than the Sishen–Saldanha and Ermelo–Richards Bay links, road freight carries more that rail (Department of Transport [DoT], 2017).

Table 2: Comparison of rail and road transportation across key routes

Route	Commodities	Rail (MT)	Road (mt)
Ermelo–Richards Bay	Coal, steel, timber, chrome	78	0
Sishen–Saldanha	Iron ore, lead	62	0
Gauteng–Durban	Containers, steel, cars, coal, manganese, fuels, perishables	24	44
Gauteng–Cape Town	Cars, grains, containers, perishables, cement, steel	11	15
Durban–Pongola	Containers, fuel, chemicals, timber	5.2	7

Route	Commodities	Rail (MT)	Road (mt)
Gauteng–Musina	Foods, fuels, vehicles, cement, perishables, beverages	4.5	12

Note: MT = rail tonne; mt = road tonne

Source: DoT (2017).

Figure 2 below illustrates the major corridors in South Africa, with the major ports indicated as filled circles, and the various corridors indicated by the colouring as per the legend. As is evident, certain ports service specific corridors, with the exception of Richards Bay, which services both the North and North East Corridors. The Cape Corridor is serviced by four ports. In addition to the freight rail, there are the pipelines to transport liquid fuel, primarily between the port of Durban and the economic hub in Gauteng (and some surrounding areas). The pipelines carry refined products, crude oil, gas, and aviation fuel. In 2019 and 2020, the pipelines carried approximately 17 750 million litres, which dropped to 13 067 million litres in 2021 (Transnet, 2021c).

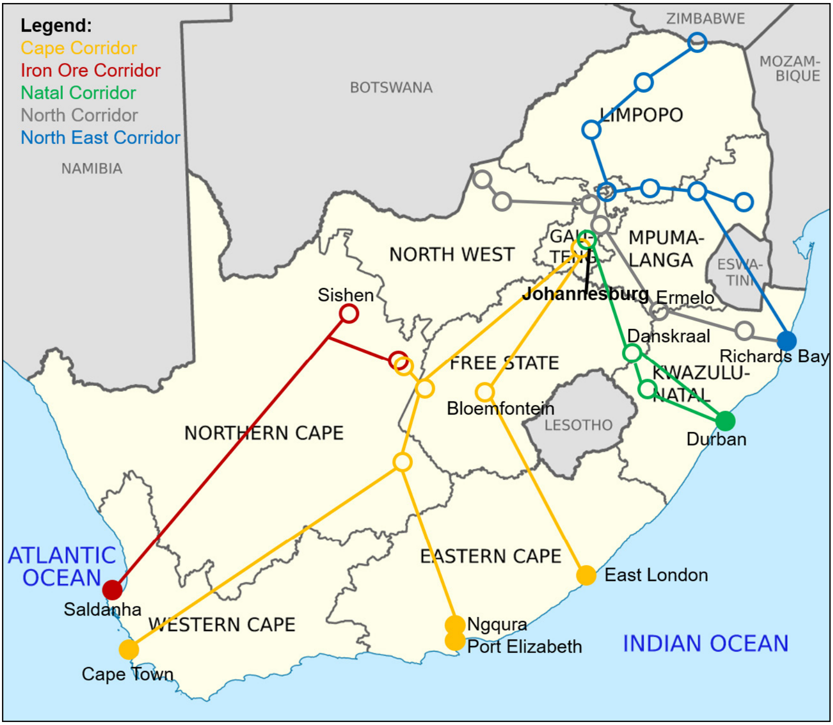

Figure 2: Major commodity corridors in South Africa

Source: Adapted from TFR (2021)

Generally, the freight rail contributes more to the GDP and revenue than the ports for break-bulk and mineral bulk. For liquid fuel, the pipelines are the major contributors, and the port terminals are the major revenue producers for containers (Transnet, 2021a). Even though the major revenue contribution by ports is through containers, they are still vital to be able to export and import other commodities, as their failure could render the railways and pipelines ineffective.

In an international context, South Africa is the world's sixth largest coal-exporting country (Mining Technology, 2020), the top supplier of chromium and manganese, the third largest supplier of Titanium minerals, the sixth largest for iron ore, and one of the major suppliers of a number of other minerals and gemstones (United States Geological Survey [USGS], 2020). This implies that South Africa might become a target of cyber operations should some country wish to disrupt the supply of certain mineral commodities.

Given the overview of the commodities and value chains in general and specific to South Africa, the next section focuses on cybersecurity for physical transport infrastructure.

Cybersecurity of physical transport infrastructure

This section discusses the classification of the physical transportation sector as critical infrastructure nationally and internationally, and reasons for targeting commodity value chains. It also provides an overview of previous notable cyber incidents affecting transportation systems globally.

Physical transportation as critical infrastructure

The US Cybersecurity and Infrastructure Security Agency (CISA) considers the transportation system sector as one of the 16 critical infrastructures, and indicates seven subsectors. Of relevance to this article are the maritime transportation system, the freight rail system, and pipelines (CISA, 2020). Previous works on critical infrastructure protection, such as Ware (1998), Nickolov (2005) and Macaulay (2008) have all considered the transportation sector as critical. Theoharidou, Kandias and Gritzalis (2012) highlight that the transport sector is particularly important for the economy. They further emphasise the interdependencies that exist with other critical infrastructure sectors. The *Australian Security of Critical Infrastructure Act (No. 29 of 2018)* explicitly considers a number of ports as critical, and in subsequent updates, of which the *Security Legislation Amendment (Critical Infrastructure Protection) Act (No. 33 of 2022)* is the latest, explicitly incorporates cybersecurity considerations as well as recognition of interdependencies amongst critical infrastructure.

From an SA perspective, section 16 of the *Critical Infrastructure Protection Act (No. 8 of 2019)* specifies that infrastructure is eligible for declaration as critical if its operation is "essential for the economy, national security, public safety and the continuous provision of basic public services", and if the loss or impairment of the infrastructure will have severe negative consequences for the country, society (in terms of safety and the law), or national security. As described above, the trade of commodities represents over 40% of the GDP; therefore, significant disruptions of the transportation sector will have a severe impact on the ability to trade in these commodities, resulting in negative impacts on the economy.

The *Critical Infrastructure Protection Act*, however, has only one reference to cybersecurity, in that at least one member of a Critical Infrastructure Council should have knowledge of cybersecurity. There is also no specified representative from the Department of Communications and Digital Technologies (DCDT), which has the mandate for the national Cybersecurity Hub (see DCDT, 2020). The National Cybersecurity Policy Framework focuses on critical information infrastructure and the establishment of sector computer security incident response teams (CSIRTs). Said framework called for the establishment of the above-mentioned Cybersecurity Hub as well as a National Cybersecurity Advisory Council (State Security Agency [SSA], 2015). At the time of writing (2022), limited sector CSIRTs have been established, and none for the transportation sector. There is no consideration of the interdependencies of various critical infrastructures in either the Critical Infrastructure Protection Act or the National Cybersecurity Policy Framework. A dated cyber security policy from 2009 however indicates the relevance of cybersecurity to critical information infrastructure, suggesting that the coordination of responses to cyber incidents against critical infrastructure is the mandate of a national CSIRT and a government CSIRT (Department of Communications [DOC], 2009); however, this does not seem to have been retained explicitly by later documents.

Physical transportation and commodity value chains as a target

For the purposes of this article, the focus is on two threat actor types: cybercriminals and nation states. Given the value of cargo and payments being made for physical transportation, cybercriminals have an opportunity to achieve large pay-outs through scams targeting the transportation sector. Ransomware is likely to be the most disruptive. The incident at the SA freight organisation Transnet illustrated the potential impact. This and other examples of incidents are discussed in more detail below.

State actors are motivated by geopolitical reasons, and targeting commodity value chains could be used to gain (or maintain) a competitive advantage in international trade over a commodity (Van Niekerk, 2019). From an international law perspective, targeting a specific terminal or rail line to affect limited commodities will not constitute an act of war, compared to disrupting major power generation or stock exchanges (Van Niekerk & Ramluckan, 2019). The targeting of commodity value chains by cyber operations was specifically proposed by Van Niekerk (2019) as a form of economic information warfare. Traditionally, economic warfare can be conducted through a number of tactics, including blockades, the disruption of supply chains, disrupting supporting infrastructure, or degrading, exploiting or corrupting economic information (Deakin, 2003; Lambert, 2017). As Lambert (2017) notes, almost immediate commodity price fluctuations may occur due to deficiencies or excesses in supply as a result of globalisation. It is therefore feasible for nations to employ a timed cyber operation to affect global supply of a commodity in order to gain a strategic advantage, such as being able to gain market share due to the disruption of a competing nation (Van Niekerk, 2019).

Cyber operations can target various points along a commodity value chain in order to cause disruptions. Focusing on a single point of failure within the commodity value chain will maximise the impact of the cyber operation to disrupt the commodity supply

(Van Niekerk, 2019). For cybercriminals, this will put pressure on the organisation to pay the ransom, and for nation states, this will result in longer recovery times to allow them to benefit from their strategic objectives. To affect a commodity value chain, a cyber operation could target the source (extraction, refinement, or manufacturing of a commodity), the transportation (rail, road, maritime and pipelines), or the human decision-making processes at corporate or national level.

To target the source or transportation, the cyber operations will need to target industrial processes containing cyber-physical systems, such as supervisory control and data acquisition (SCADA) systems. In such a scenario, a cyber incident may affect conveyer belts, gantry cranes, refineries, switching on the railways, sea-going vessels, or other related equipment. Analysis by Van Niekerk (2017) and Van Niekerk and Ramluckan (2019) indicated that – given the number of cyber incidents affecting industrial processes and the transportation sector – it is feasible, although still rare, for cyber operations to cause sufficient physical disruption. With increased digitisation, the Industrial Internet of Things (IIoT) is becoming pervasive and is being introduced into the transport sector (for example, automated ports). The IIoT provides opportunities for organisations to improve operational efficiencies, but also introduces security risks that can be exploited by malicious cyber actors (Pretorius & Van Niekerk, 2020).

In addition to the industrial processes that directly degrade the operational capability of the infrastructure, a cyber incident affecting the supporting enterprise IT infrastructure and decision-making information could cause disruptions in commodity supply. For example, deleting legitimate orders, injecting false orders, or changing order quantities, could not only cause conflict between suppliers and consumers, but could also result in surplus or shortages of supply. Scheduling systems could be corrupted so that insufficient equipment or transportation would be available when needed, or equipment does not undergo required maintenance. Corrupting other business information to alter decision-making or corrupting individuals directly to make poor decisions could also have a long-term degrading effect (Van Niekerk & Ramluckan, 2019). A cyber incident affecting the broader enterprise IT network could potentially achieve several of the above-mentioned consequences by denying executives and operations personnel access to the systems they need to make decisions or conduct daily operations.

The sections below will reflect a discussion on a number of cyber incidents to illustrate the susceptibility and consequences of these incidents in the transportation sector.

Maritime cybersecurity incidents

Of the 51 cyber incidents targeting physical transportation sector analysed by Van Niekerk (2017), 25 affected the maritime subsector, and eight resulted in denial of services or disruption of operations.

Notable incidents affecting port and vessel operations globally include:

- In 2001, a hacker used vulnerable servers in the Port of Houston to conduct a denial-of-service attack, which crashed the servers and disrupted port operations (McCue, 2003).
- In 2009, safety systems on three oil rigs were disabled by a disgruntled employee (Kravets, 2009).
- Royal Navy NavyStar/N* systems aboard warships were infected by the Conficker worm (Kirk, 2009; Page, 2009).
- In 2012, organised crime monitored shipping containers they were using by gaining unauthorised access to cargo systems operated by Australian Customs (CyberKeel, 2014).
- An oil rig navigation system was infected with malware, resulting in it drifting off position (Knox, 2015; Swanbeck, 2015).
- In 2013, smugglers used remote access devices to gain unauthorised access to systems in the Port of Antwerp to monitor their containers (Dunn, 2013).
- In 2014, hackers tilted an oil rig off East Africa, stopping operations for a week, and malware rendered another oil rig unseaworthy for almost three weeks (CyberKeel, 2014; Wagstaff, 2014).
- In 2015, operations at a European port were disrupted for 12 hours due to the GPS signals being jammed (Knox, 2015).
- The NotPetya ransomware worm severely disrupted global operations of Maersk, including affecting port operations. The incident was estimated to have a 300 million dollar impact (Greenberg, 2018).
- It was reported that in 2017, at least 20 vessels experienced potential GPS and AIS spoofing in the Black Sea (Hambling, 2017).
- In 2019, irregular GPS and Automatic Identification System (AIS) readings as well as GPS jamming were reported at the Port of Shanghai (Goward, 2019).
- In 2020, operations at the Shahid Rajaee terminal in Iran were disrupted by a cyberattack, attributed to an Israeli response to an alleged Iranian cyber operation against an Israeli water system (Warrick & Nakashima, 2020).
- In 2021, SA port terminal operations were disrupted by ransomware (Gallagher & Burkhardt, 2021; Ginindza, 2021; Njini & Viljoen, 2021).

Of the 14 incidents described above, seven affected port operations, six affected vessels, and one affected both. Two of these incidents were in Africa, illustrating that the continent is also affected by maritime cybersecurity incidents. In addition to the above, incidents of traditional cybercrime affecting maritime organisations, such as scams, phishing attempts and fraudulent bank account changes were reported. Some instances of cyber espionage were also apparent (Meland et al., 2021; Park, Shi, Zhang, Kontovas & Chang, 2019; Van Niekerk, 2017). There have been additional instances of ransomware impacting on the IT networks of shipping companies and ports; however, these affected corporate services and functionality (including bookings), but not operational systems (Meland et al., 2021; Park et al., 2019). There have been instances of researchers demonstrating possible vulnerabilities in on-board systems, such as the Electronic Chart Display and Information Systems, Voyage Data Recorders and satellite communication, as well as possible attacks, such as spoofing GPS and AIS (Van Niekerk, 2017). Reports of spoofed locations for warships have been reported since 2020 (Harris, 2021).

From the incidents described, it is possible to affect both the systems of the ports to disrupt operations, or to disrupt vessel navigation nearby a port to make navigation hazardous. Berthed vessels could be rendered unseaworthy by malware, thereby blocking berthing places in a port. While this article focuses on a high-level perspective of whether cyber incidents could affect commodity value chains, two incidents are worth a more detailed discussion due to the scale of the disruptions: the NotPetya ransomware affecting Maersk, and the Transnet ransomware incident. For Maersk, the incident disrupted at least 17 terminals across three continents, trucks had to be turned away at the terminals, and cranes were not operational. Systems on board ships were not affected, but the terminals were unable to process the EDI files to determine the cargo that needed to be loaded or unloaded from the vessels. The organisation had to rebuild over 4 000 servers and 45 000 personal computers, including 150 domain controllers, and reinstall 2 500 applications. Luckily, a single domain controller in Ghana survived, as it was offline due to a power outage (Cimpanu, 2018; Greenberg, 2018).

In the Transnet case, the incident occurred with very bad timing. It was a week after major protests had disrupted rail operations, and was also at a key time for exporting citrus fruit (Ash, 2021; Smith, 2021; Toyana, 2021). As with the Maersk incident, it was difficult to track containers in the ports, and some ships opted to reroute elsewhere as the incident continued for a week, and some manual operations and booking were in put in place (Ash, 2021). There were also concerns that employee salaries would not be paid, resulting in threats of employees striking. Combined with the protests, there was an approximately 12-day impact on truck freight (Toyana, 2021).

Rail cybersecurity incidents

Railways are increasingly being affected by cyber incidents, including DDoS (distributed denial of service), data breaches, malware and ransomware (Macola, 2021), and threat actors include both cybercriminals and state actors (Fletcher & Bye, 2022).

- In 2008, tram carriages were derailed in Poland after a teenager had built a device to switch points of the tram lines remotely (Ismail, Sitnikova & Slay, 2015; Leyden, 2008).
- In 2013, train delays resulted from a malware infection at the CSX Corporation, (Miller & Rowe, 2012).
- In 2011, a network intrusion at a United States (US) railway affected signals over two days resulting in train delays (Ragan, 2012; Sternstein, 2012).
- In 2016, a passenger rail service in San Francisco was disrupted for two days as many systems were taken offline as a precautionary measure during a ransomware incident (Fletcher & Bye, 2022).
- A Danish train operator suffered disruptions in 2018 due to a DDoS attack, which prevented the purchase of tickets (Fletcher & Bye, 2022; Hill, 2018).

- In 2022, multiple claims emerged that hacktivists called 'Cyber Partisans' affected Belarussian Railways to delay Russian troop movements; these include ransomware attacks against databases and disrupting its ticketing services (Greenberg, 2022), and affecting traffic control systems (Smeets & Achberger, 2022). This was followed by similar claims from the Anonymous collective (Paganini, 2022).
- A ransomware attack affected ticking systems in Italy in March 2022 (Goodman, 2022).

In addition to interference in the maritime industry, examples of scams, fraudulent changes to bank accounts, ransomware, and cyber espionage are available (Fletcher & Bye, 2022); however, these did not affect operations. In 2016, security researchers demonstrated that railway systems are vulnerable, referring to collision avoidance systems and other control systems that could provide a means for cyber operators to derail trains (Pauli, 2016). Reports in 2022 indicated that railway safety systems are still vulnerable (Zukowski, 2022). While many of these incidents do not specifically involve freight rail, the possibility of remotely affecting signals, switching points, and other controls indicate that disruptions to freight rail are possible.

Pipeline and liquid fuel cybersecurity incidents

Key cyber incidents impact on liquid fuel organisations and pipelines include:

- In 1999, flow control systems at Gazprom were reportedly accessed by attackers using backdoors and with aid of a disgruntled insider (Miller & Rowe, 2012).
- From December 2011 to June 2012, 23 pipeline operators in the United States had operational documentation stolen in an apparent cyber-espionage campaign (Clayton, 2013).
- In 2012, the Saudi Aramco oil company was affected by a 'wiper' malware called Shamoon that corrupted files and computer hard drives to make them unusable. Approximately 30 000 computers were affected, and it took the company two weeks to recover. There were however no indications that industrial systems were directly affected (Bronk & Tikk-Ringas, 2013).
- In 2021, shortly after the Saudi Aramco incident, Qatari RasGas was affected by malware on its corporate network (Mills, 2012).
- In May 2021, Colonial Pipelines (United States) was affected by ransomware. While the pipeline systems were not infected, they were shut-down to prevent infection. The incident resulted in the declaration of a state of emergency by the US president, panic buying of petrol and shortages of aviation fuel (Kerner, 2022).

A notable point in terms of the above incidents is that reports indicate pipeline control systems were accessed remotely, and that the ransomware at Colonial Pipelines did affect operations indirectly, with noticeable social impact in the surrounding areas.

Other relevant cyber incidents

In addition to the cyber incidents described above, a few others are relevant to the discussion in this article:

- malware affected the monitoring of process in an SA chemical plant (Cusimano, 2010);
- the Stuxnet worm affected the control systems, particularly the centrifuges at an Iranian nuclear enrichment facility (Zetter, 2014);
- a cyber incident resulted in an explosion at a German steel mill (Cohen, 2021);
- parts of the Ukraine power grid was shut down by a cyber operations (Greenberg, 2017); and
- a key Israeli toll road was affected by malware (Ashford, 2013).

These incidents indicate that processing facilities that could form part of a value chain, but outside of the transportation infrastructure, are also susceptible to cyber disruption. When a key processing facility is unable to produce the commodity for shipment, then the transportation infrastructure cannot generate revenue for the commodities.

Initiatives and best practices for transportation cybersecurity

Industry and government initiatives internationally have focused on strengthening cybersecurity for physical transportation. In particular, the American Transportation Security Agency (TSA) (2022) released a cybersecurity toolkit for surface transportation in 2021 with a number of guiding documents. A multi-national project in Europe, 4SECURAIL (2022), seeks to develop cybersecurity for the railway sector. The International Maritime Organization (IMO) (2019) provides guidelines for managing cybersecurity within this sector. In 2021, the Atlantic Council's Cyber Statecraft Initiative released a report on maritime security, which considered the lifecycle of ships, key aspects of ports, and the cargo lifecycle (Loomis et al., 2021).

While only a few initiatives have been mentioned, it is important to note that there are dedicated programmes and initiatives addressing the challenges and providing guidance.

Analysing the susceptibility of South African commodity value chains to cyber incidents

This section combines the information in the previous two sections to illustrate possible points of failure within the commodity value chains in South Africa.

In Table 1 above, it was shown that agricultural commodities are primarily handled by Cape Town (50% of capacity) followed closely by Durban. The container sector is mostly handled by Durban with 49% of the handling capacity, followed by Ngqura with 27%. Durban handles the vast majority of the automotive sector with 64% handling of cargo. Saldanha is responsible for the vast majority of the mineral bulk with 65% of capacity and handles the majority of the iron ore. This is followed by Richards Bay with 29%, handling the majority of the coal and servicing two of the major rail corridors. Saldanha handles the majority of break bulk (48%), followed by Durban (24%).

The top two rail routes depicted in Table 2 service coal and iron ore, but do not exhibit any major alternative road transportation. This indicates the considerable impact a failure of those rail routes will have on the respective commodities. The third major rail route, between Gauteng and Durban, only carries 36% of the cargo and the road carries the majority. In addition, there are two routes between Durban and Danskraal, giving a degree of redundancy. The major ports, rail routes, and their approximate influence on the GDP is illustrated in Table 3 and Figure 2. The word 'influence' is chosen as the railways contribute more than the ports for many mineral and bulk commodities; however, the ports are a major means of exporting, therefore without them the railways will be significantly less effective.

Table 3: Key ports and rail routes for major commodities

Commodity	Key port		Key rail route	Approx. port impact on GDP (%)
	Port	Approx. cargo handled (%)		
Agriculture	Cape Town	50		
Containers	Durban	50	Gauteng–Durban	~6
Automotive	Durban	64		~4.2
Coal	Richards Bay	~100	Ermelo–Richards Bay	3
Iron ore	Saldanha	~100	Sishen–Saldanha	1.5
Liquid fuels	Durban	~100		

Source: Author's own compilation based on data in Tables 1 and 2

From the above, it is evident that the port of Durban is the most critical: it has an impact of at least 10% of the GDP, and dominates the automotive, container and liquid fuel commodities, with meaningful impact on the agricultural and break-bulk commodities. Richard's Bay handles the majority of coal, of which South Africa is sixth highest exporter in the world, and services two major rail routes. It has an impact of approximately 3% of the GDP. Saldanha handles the majority of iron ore (of which SA is the sixth largest producer) and break-bulk, with an impact approximately 1.5% of the GDP. Cape Town handles approximately half the agricultural bulk, which is listed as a key factor in Transnet's economic recovery plan (Transnet, 2021a).

Two systems that are mentioned for SA ports are relevant to the incidents: Navis and EDI. EDI was specifically mentioned in the above example of the NotPetya infection of the Maersk systems. Both the Maersk and Transnet examples indicated that container tracking and moving were hindered by the cyber incidents, which is the function the Navis systems also performs. As indicated above, there is a single instance of the system managing all container terminals across the country. A localised cyber incident could therefore potentially affect the ability of the entire country to manage container shipments. It should be noted that the Navis system itself does not need to be targeted directly, but if the localised network is degraded due to a cyber incident or if the Navis system is taken offline as a precautionary measure (as in the Colonial Pipelines incident), the impact will be the same as when the system is targeted.

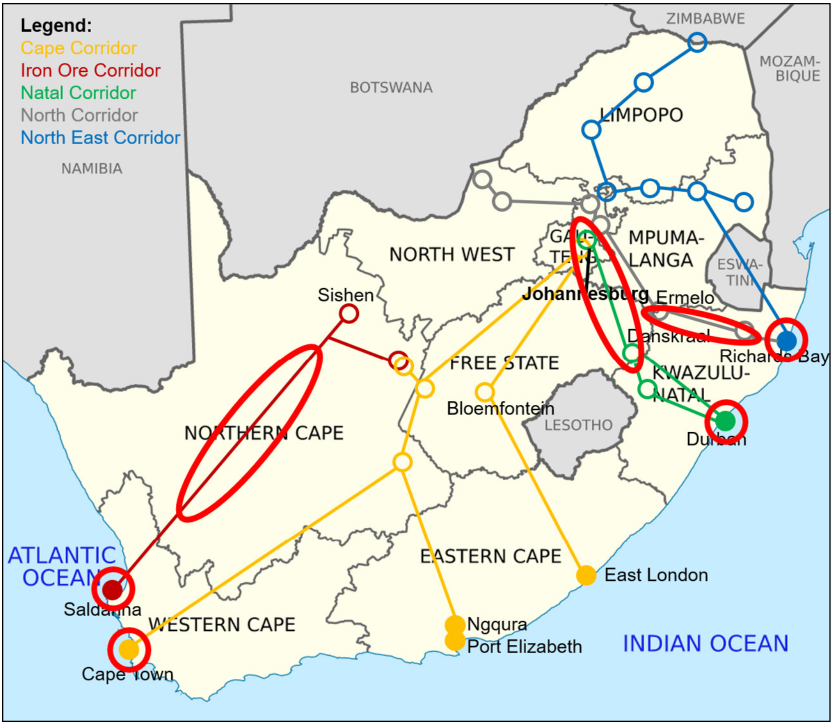

Figure 3: High-level single points of failure in rail and maritime transportation

Source: Adapted from TFR (2021)

Hypothetical examples

To illustrate the potential susceptibility, two hypothetical examples are used: one considering a cybercrime incident and the second, a more targeted state actor scenario. The two scenarios are presented, and then a comparative analysis is provided.

Scenario 1: Cybercrime

For this scenario, an evolution of ransomware attacks, known as a 'triple extortion attack' is considered. Triple extortion uses three methods to maximise the success of forcing the target to pay the ransom, namely ransomware, and the threat of leaking exfiltrated data, enhanced with either DDoS or directly extorting clients or customers based on the exfiltrated data (Snowden, 2021). The scenario will take a worst-case approach to illustrate what is possible. The first stage is the initial infection, which will exfiltrate data and then update to deploy the ransomware. The ransomware affects the servers managing the network, disrupting key services – such as train scheduling, container tracking, and berthing for vessels – resulting in delays as each vessel request needs to be verified. Some services – such as the website, external EDI with organisations, and booking portals – are at this stage still unaffected. This phase however causes major disruptions for containers vessels and transportation, delays for bulk commodities, and reputation damage for the organisation and nation. The port of Durban was particularly hard hit, being one of the largest terminals, and trucks were backed up on the roads causing discontent and inconvenience for surrounding residents.

The second phase then launches a DDoS attack to hinder the remaining services – such as booking and EDI – further disrupting the ability of the organisation and clients to engage with one another. This causes further reputational damage due to the worsening situation, and the inability to make bookings threatens the future operation of the commodity value chains.

The third phase threatens to release exfiltrated data, initially private to the organisation. Even if the organisation has recovered from the ransomware and DDoS, this phase is still a significant threat. If unsuccessful, extortion attempts against client organisations are attempted, with the potential to release contracting and preferential rate information (if any), or labour brokering information. The release of this information will cause discontent, and clients react strongly against the organisation. The compromise of the data leaks to the media, possibly from one of the clients, triggering an investigation under the national privacy laws. The reputation of the organisation is shattered, eroding international and local confidence in its ability to deliver services and protect customer data. Many shipping organisations will therefore choose to use alternative commodity corridors into the continent.

Scenario 2: State actor

This scenario considers a more targeted and persistent attack focusing on a specific commodity. Nation A has discovered deposits of iron ore and is trying to strengthen its market share for the commodity. To facilitate this, Nation A endeavours to use cyber operations to degrade the ability of competing nations to export iron ore. As South Africa is of similar international standing for providing the commodity, it is one of the countries targeted. The cyber operation is stealthy, and disrupts computers and industrial control systems throughout the iron ore value chain. In particular, power distribution to the mines at Sishen, the port of Saldanha, and the connecting railways are affected. Industrial control systems at the conveyor belts and loading equipment are affected to induce erratic behaviour making the equipment unusable, and, the switching of the tracks are disrupted causing a derailment. The key bottleneck will be the port of Saldanha, as well as its associated rail route. The focus is on disrupting these, where different areas can be affected at different times to create a prolonged effect. This affects the iron ore supply, which in turn affects commodity pricing, allowing Nation A to gain additional market share as well as making it possible for Nation A to sell at a higher price. Once Nation A has established itself as a supplier of iron ore by disrupting South African and other suppliers, the cyber operations cease.

Scenario comparison

The cybercrime scenario gives rise to a broader outcome, which could affect multiple commodities. Here, the goal is to force the organisation into paying, therefore as much pressure as possible will be leveraged: an increase in the number of commodities that are affected translates into more pressure. The implications are far-reaching, particularly in terms of reputational damage of the organisation targeted, and especially for South Africa as a major destination for trade into Africa. This will have both short- and long-term impacts on the national economy and, by extension, on society. By comparison, a state actor will aim to be stealthier and more precise to achieve a specific objective. The reputational damage will be more limited, particularly if multiple nations are targeted. In addition, the cyber operation is likely to be more persistent until the objectives are achieved or the operation can no longer be continued. It is possible that an emerging state actor would use apparent cybercriminal tactics causing more widespread 'collateral' damage, as the tools and/or services can be procured more easily than developing a dedicated in-house process to target specific cyber-physical systems, and using more readily available code will aid in avoiding attribution.

Summary and recommendations

The article has illustrated some critical value chains for which there is limited redundancy, and can be particularly susceptible to disruption via cyber operations. In addition, these routes contribute to the GDP as well as significant proportions of international supply of the commodities. The port of Durban features as a key entry point into the country, and major disruptions of the port could have significant economic consequences for South Africa but could also disrupt global shipping around the continent. The ports of Richards Bay (coal) and Saldanha (iron ore) are also important, along with associated rail routes. The port of Cape Town is important for the growth of the agriculture sector. Two hypothetical scenarios reflecting cybercrime and cyber operations illustrated the potential for disruption of trade corridors in the country. However, while these scenarios are hypothetical, it should be noted that South Africa has already experienced a similar scenario in 2021, and other ports have experienced disruption due to activities in cyberspace.

From the literature it is apparent that, compared to other nations, South Africa does not yet have sufficient formalised structures in place nationally or within the sector to respond to and recover from major cyber incidents, and there appears to be a disjuncture between cybersecurity and critical infrastructure protection. As South Africa is a one of the top suppliers of raw materials and has notable automotive and agricultural sectors, it is imperative that measures be taken to strengthen cybersecurity in the transportation sector. Recommendations for improvement are provided in the section below.

This study was limited to the strategic setting, and consequently did not consider specific technologies or technical vulnerabilities. While the scenarios and discussion focused on South Africa, the high-level premises can be modified to apply to other nations.

Recommendations

Measures to improve cyber resiliency for the freight transportation sector can be implemented or enhanced at national, sectoral and organisational levels. The recommendations considered here were drawn from existing incidents, best practices, and the analysis of the South African (SA) scenario. At a national level, the relevant legislation needs to be reviewed and updated regularly. In particular, cybersecurity needs to feature more prominently in the *Critical Infrastructure Protection Act (8 of 2019)*. In addition, there needs to be greater integration of the National Cyber Security Advisory Council and the Critical Infrastructure Council. A specific agency can be established, similar to the US Cybersecurity and Infrastructure Security Agency.

At a sector level, it is imperative to establish a sector-based computer security incident response team (CSIRT) or a similar facility to aid in responding to incidents and reducing response and recovery time. In addition, the CSIRT could perform other functions, such as distributing alerts, coordinating with other sectors, and facilitating coordination within the physical transport sector. A set of frameworks and standards for cybersecurity best practice within the sector (or for each sub-sector) should be established. Alternatively, existing international frameworks could be adopted formally. In this endeavour, it will be important to engage with international forums and working groups developing cybersecurity best practices for physical transportation. Specialist skills or job profiles for cybersecurity professionals in the sector should be identified, for example industrial control system security.

At an organisational level, there also needs to be engagement with the relevant national and international forums, and particular collaboration with sector cybersecurity functions. Organisations should be responsible for ensuring there is adequate staffing with the necessary general and specialist cybersecurity skills. The specific skill set and job profiles required can be drawn from the sector recommendations. In addition, the organisations should be responsible for conducting strategic and technical risk and vulnerability assessments on their segments of value chains to identify single points of failure and critical assets, and should then implement appropriate security control measures according to sector best practices. It will be important to implement cyber crisis response exercises for organisations to understand their roles in a national cyber crisis, particularly one involving the transport sector.

From an academic perspective, future research could provide more detail on the specific technical vulnerabilities that may be present within the transportation sector, and could consider the level of cybersecurity awareness amongst employees. These future studies could be integrated with the strategic perspective to provide a more holistic view of cybersecurity in the sector.

Conclusion

Cybersecurity threats have affected the physical transport sector, and the maritime sector was hit particularly hard. The current considered the susceptibility of commodity SA supply chains to disruptions from cyber incidents at a strategic level, with the aim of identifying key areas that may prove to be a single point of failure. SA ports have already experienced a significant cyber incident in 2021; therefore, the feasibility has already been demonstrated. The port of Durban is of particular importance, as it handles close to 50% of container and automotive cargo, as well as a notable percentage of other commodities. The ports of Richards Bay and Saldanha are important for certain bulk commodities, as are the associated rail routes. Cape Town is important for the agricultural sector.

Two hypothetical scenarios illustrated that cybercriminal activity may be more damaging and might affect multiple commodities. Targeted state-backed operations could however limit the effect on specific commodities, but be more persistent in the disruption. It is recommended that national laws be updated to foster good alignment with cybersecurity and critical infrastructure protection. The sector should also engage with relevant forums to implement or adopt best practice frameworks or standards to improve resiliency of the sector.

About the Author

Prof Brett van Niekerk (PhD) is an associate professor in the Department of Information Technology at the Durban University of Technology, a non-resident fellow at the Security Institute for Governance and Leadership in Africa (Stellenbosch University), chairs the International Federation of Information Processing Working Group on ICT in Peace and War, and is Editor-in-Chief of the International Journal of Cyber Warfare and Terrorism. He has cybersecurity experience across industry, academia and civil society. He has actively participated in international cybersecurity forums (Global Commission on the Stability of Cyberspace, Paris Call working groups, Carnegie Endowment for International Peace's project on countering influence operations). He is CISM certified, with over 50 academic publications and 20 presentations at industry events.

References

4SECURAIL. 2022. *Formal methods and CSIRT for the railway sector*. Available at: <https://www.4securail.eu/> [Accessed 15 June 2022].

Ash, P. 2021. Cargo ships give SA a wide berth in wake of cyber attack. *Time Live*, 27 July. Available at: <https://www.timeslive.co.za/news/south-africa/2021-07-27-cargo-ships-give-sa-a-wide-berth-in-wake-of-cyber-attack/> [Accessed 1 June 2022].

Ashford, W. 2013. Cyber attack shuts down Israeli toll road tunnel. *Computer Weekly*, 28 October. Available at: <https://www.computerweekly.com/news/2240207924/Cyber-attack-shuts-down-Israeli-toll-road-tunnel> [Accessed 15 June 2022].

Australian Government. 2018. *Security of Critical Infrastructure Act 2018*. Available at: <https://www.legislation.gov.au/Details/C2018A00029/Download> [Accessed 25 May 2022].

Australian Government. 2022. *Security Legislation Amendment (Critical Infrastructure Protection) Act 2022*. Available at: <https://www.legislation.gov.au/Details/C2022A00033> [Accessed 25 May 2022].

Britannica. 2023. *Anonymous*. Britannica. Available at: <https://www.britannica.com/topic/Anonymous-hacking-group> [Accessed 30 November 2023].

Bronk, C. & Tikk-Ringas, E. 2013. The cyber attack on Saudi Aramco. *Survival*, 55(2), 81–96.

Carman, N. 2023. The use of labour brokers. Labour Guide. Available at <https://labourguide.co.za/general/the-use-of-labour-brokers> [Accessed 30 November 2023].

Cimpanu, C. 2018. *Maersk reinstalled 45,000 PCs and 4,000 servers to recover from NotPetya attack.* BleepingComputer. Available at: <https://www.bleepingcomputer.com/news/security/maersk-reinstalled-45-000-pcs-and-4-000-servers-to-recover-from-notpetya-attack> [Accessed 7 September 2018].

CISA (Cybersecurity and Infrastructure Security Agency). 2020. *Transportation systems sector*. Available at: <https://www.cisa.gov/transportation-systems-sector> [Accessed 24 May 2022].

Clayton, M. 2013. *Exclusive: Cyberattack leaves natural gas pipelines vulnerable to sabotage*. The Christian Science Monitor. Available at: <https://www.csmonitor.com/Environment/2013/0227/Exclusive-Cyberattack-leaves-natural-gas-pipelines-vulnerable-to-sabotage> [Accessed 3 June 2022].

Cohen, G. 2021. *Throwback attack: A cyberattack causes physical damage at a German steel mill*. Industrial Cybersecurity Pulse. Available at: <https://www.industrialcybersecuritypulse.com/throwback-attack-a-cyberattack-causes-physical-damage-at-a-german-steel-mill/> [Accessed 16 June 2022].

Cusimano, J. 2010. DCS virus infection, investigation and response: A case study. Presentation to Industrial Control Systems Joint Working Group (ICSJWG) Fall Conference, 25–28 October, Seattle, WA.

CyberKeel. 2014. *Maritime cyber-risks: Virtual pirates at large on the cyber seas*. Available at: <http://www.cyberkeel.com/images/pdf-files/Whitepaper.pdf> [Accessed 2 November 2016].

DCDT (Department of Communications and Digital Technologies). 2020. *Cybersecurity Hub Project.* Available at: <https://www.dcdt.gov.za/cybersecurity-hub-project.html> [Accessed 25 May 2022].

Deakin, R.L. 2003. Economic information warfare: Analysis of the relationship between the protection of financial information infrastructure and Australia’s national security. Unpublished MA dissertation, Queensland University of Technology.

DOC (Department of Communications). 2009. *Cybersecurity Policy of South Africa*. Available at: <https://www.ellipsis.co.za/wp-content/uploads/2011/02/CYBER-SECURITY-POLICY-draft.pdf> [Accessed 26 September 2022].

DoT (Department of Transport). 2017. *Chapter 7: Freight transport*. Available at: <https://www.transport.gov.za/documents/11623/39906/7_FreightTransport2017.pdf/a3f7cb55-8d77-4eea-b665-4c896c95a0d8> [Accessed 20 May 2022].

Dunn, J.E. 2013. Hackers planted remote devices to smuggle drugs through Antwerp port, Europol reveals. *Techworld*, 16 October. Available at: <http://news.techworld.com/security/3474018/hackers-planted-remote-devices-to-smuggledrugs-through-antwerp-port-europol-reveals/> [Accessed 2 November 2016].

E-International Relations. 2021. Positivism, Post-Positivism and Interpretivism. 25 September. Available at: <https://www.e-ir.info/2021/09/25/positivism-post-positivism-and-interpretivism/> [Accessed 30 November 2023].

Fletcher, D. & Bye, P. 2022. *Cybersecurity in transit systems*. The National Academies Press. Available at: <https://nap.nationalacademies.org/catalog/26475/cybersecurity-in-transit-systems> [Accessed 27 May 2022].

Gallagher, R. & Burkhardt, P. 2021. 'Death Kitty' ransomware linked to South African port attack. *Bloomberg*, 29 July. Available at: <https://www.bloomberg.com/news/articles/2021-07-29/-death-kitty-ransomware-linked-to-attack-on-south-african-ports> [Accessed 3 January 2022].

Ginindza, B. 2021. Transnet 'cyber attack' causes logistics logjam from road to freight and ports. *IOL*, 23 July. Available at: <https://www.iol.co.za/business-report/economy/transnet-cyber-attack-causes-logistics-logjam-from-road-to-freight-and-ports-56f6bd97-c5ef-4d65-90d6-c41d0fe290e2> [Accessed 17 May 2022].

Goodman, M. 2022. Italian railways attacked by ransomware: Ticket sales stopped. *Research Snipers*, 24 March. Available at: <https://researchsnipers.com/italian-railways-attacked-by-ransomware-ticket-sales-stopped/> [Accessed 28 March 2022].

Goward, D. 2019. GPS jamming and spoofing reported at port of Shanghai. *The Maritime Executive*, 13 August. Available at: <https://www.maritime-executive.com/editorials/gps-jamming-and-spoofing-at-port-of-shanghai> [Accessed 27 May 2022].

Greenberg, A. 2017. How an entire nation became Russia's test lab for cyberwar. *Wired*, 20 June. Available at: <https://www.wired.com/story/russian-hackers-attack-ukraine/> [Accessed 15 June 2022].

Greenberg, A. 2018. The untold story of NotPetya, the most devastating cyberattack in history. *Wired*, 22 August. Available at: <https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/> [Accessed 27 May 2022].

Greenberg, A. 2022. Why the Belarus railways hack marks a first for ransomware. *Wired*, 25 January. Available at: <https://www.wired.com/story/belarus-railways-ransomware-hack-cyber-partisans/> [Accessed 27 May 2022].

Hambling, D. 2017. Ships fooled in GPS spoofing attack suggest Russian cyberweapon. *New Scientist*, 10 August. Available at: <https://www.newscientist.com/article/2143499-ships-fooled-in-gps-spoofing-attack-suggest-russian-cyberweapon/> [Accessed 27 May 2022].

Harris, M. 2021. Phantom warships are courting chaos in conflict zones. *Wired*, 29 July. Available at: <https://www.wired.com/story/fake-warships-ais-signals-russia-crimea/> [Accessed 27 May 2022].

Hill, M. 2018. Danish railway company DSB suffers DDoS attack. *Infosecurity Magazine*, 14 May. Available at: <https://www.infosecurity-magazine.com/news/danish-railway-ddos-attack/> [Accessed 27 May 2022].

IMO (International Maritime Organization). 2019. *Maritime cyber risk*. Available at: <https://www.imo.org/en/OurWork/Security/Pages/Cyber-security.aspx> [Accessed 15 June 2022].

Ismail, S., Sitnikova, E. & Slay, J. 2015. SCADA systems cyber security for critical infrastructures: Case studies in the transport sector. In *Proceedings of the 10th International Conference on Cyber Warfare and Security (ICCWS 2015).* Reading: ACPI, 425–433.

Kerner, S.M. 2022. Colonial pipeline hack explained: Everything you need to know. *TechTarget*, 26 April. Available at: <https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know> [Accessed 2 June 2022].

Kirk, J. 2009. Virus attacks Ministry of Defence. *CIO*, 19 January. Available at: http://www.cio.co.uk/news/3460/virus-attacks-ministry-of-defence/> [Accessed 19 October 2010].

Knox, J. 2015. *Coast guard commandant on cyber in the maritime domain*. US Coast Guard. Available at: <https://mariners.coastguard.blog/2015/06/15/6152015-coast-guard-commandant-on-cyber-in-the-maritime-domain/> [Accessed 27 May 2022].

Kravets, D. 2009. Feds: Hacker disabled offshore oil platforms' leak detection system. *Wired*, 18 March. Available at: <https://www.wired.com/2009/03/feds-hacker-dis/> [Accessed 27 May 2022].

Lambert, N.A. 2017. Brits-Krieg: The strategy of economic warfare. In G. Perkovich & A.E. Levite (eds.). *Understanding cyber conflict: 14 analogies.* Washington, DC: Georgetown University Press, 123–146.

Leyden, J. 2008. Polish teen derails tram after hacking train network. *The Register*, 11 January. Available at: <http://www.theregister.co.uk/2008/01/11/tram_hack/> [Accessed 27 May 2022].

Loomis, W., Singh, V.V., Kessler, G.C. & Bellenkens, X. 2021. *Raising the colours: Signalling for cooperation on maritime cybersecurity.* Washington, DC: Atlantic Council.

Macaulay, T. 2008. *Critical infrastructure*. Boca Raton, FL: CRC Press.

Macola, I.G. 2021. Is cybersecurity in rail more important now than ever? *Railway Technology*, 29 April. Available at: <https://www.railway-technology.com/analysis/is-cybersecurity-rail-important-now-ever/> [Accessed 27 May 2022].

McCue, A. 2003. 'Revenge' hack downed US port systems. *ZDNet*, 7 October. <http://www.zdnet.com/article/revenge-hack-downed-us-port-systems/> [Accessed 27 May 2022].

Meland, P.H., Bernsmed, K., Wille, E., Rodseth, O.J. & Nesheim, D.A. 2021. A retrospective analysis of maritime cyber security incidents. *TransNav: The International Journal on Marine Navigation and Safety of Sea Transportation*, 15(3), 519–530.

Miller, B. & Rowe, D.C. 2012. A survey of SCADA and critical infrastructure incidents. Paper presented at the ACM Special Interest Group on Information Technology Education (SIGITE) Research in IT Conference, 11–13 October, Alberta.

Mills, E. 2012. Virus knocks out computers at Qatari gas firm RasGas. *CNET*, 30 August. Available at: <https://www.cnet.com/news/privacy/virus-knocks-out-computers-at-qatari-gas-firm-rasgas/> [Accessed 3 June 2022].

Mining Technology. 2020. *Coal giants: The world's biggest coal producing countries*. Available at: <https://www.mining-technology.com/analysis/featurecoal-giants-the-worlds-biggest-coal-producing-countries-4186363/> [Accessed 31 May 2022].

Moore, M.R. 2018. Exploring critical infrastructure single point of failure analysis (SPFA) for data center risk and change management. Unpublished PhD dissertation, Northcentral University.

NAVIS. 2021. *N4 Terminal Operating System*. Available at: <https://www.navis.com/en/products/terminal-operations/n4-terminal-operating-system#> [Accessed 26 September 2022].

Nickolov, E. 2005. Critical information infrastructure protection: Analysis, evaluation and expectations. *Information and Security*, 17:105–119.

Njini, F. & Viljoen, J. 2021. Transnet declares force majeure at SA ports over cyberattack. *News24*, 27 July. Available at: <https://www.news24.com/fin24/companies/transnet-declares-force-majeure-at-sa-ports-over-cyber-attack-20210727> [Accessed 17 May 2022].

Paganini, P. 2022. The anonymous hacker collective claims to have breached the Belarusian railway's data-processing network. *Security Affairs*, 27 February. Available at: <https://securityaffairs.co/wordpress/128486/hacktivism/anonymous-breached-belarusian-railways.html> [Accessed 18 March 2022].

Page, L. 2009. MoD networks still malware-plagued after two weeks. *The Register*, 20 January. Available at: <https://www.theregister.com/2009/01/20/mod_malware_still_going_strong> [Accessed 27 May 2022].

Park, C., Shi, W., Zhang, W., Kontovas, C. & Chang, C. 2019. Cybersecurity in the maritime industry: A literature review. In *Proceedings of the International Association of Maritime Universities (IAMU) Conference.* Tokyo: IAMU, 79–86.

Pauli, D. 2016. Irked train hackers talk derailment flaws, drop SCADA password list. *The Register*, 4 January. Available at: <http://www.theregister.co.uk/2016/01/04/irked_train_hackers_talk_derailment_flaws_drop_scada_password_list/> [Accessed 27 May 2022].

Porter, M.E. & Millar, V.E. 1985. How information gives you competitive advantage. *Harvard Business Review*, July. Available at: <https://hbr.org/1985/07/how-information-gives-you-competitive-advantage> [Accessed 10 September 2018].

Pretorius, B.H. & Van Niekerk, B. 2020. Industrial Internet of Things security for the transportation infrastructure. *Journal of Information Warfare*, 19(3), 50–67.

Ragan, S. 2012. Railway network disrupted after cyber attack, report says. *Security Week*, 25 January. Available at: <http://www.securityweek.com/railway-network-disruptedafter-cyber-attack-report-says> [Accessed 2 November 2016].

RSA (Republic of South Africa). 2019. *Critical Infrastructure Protection Act 2019*. Available at: <https://www.gov.za/sites/default/files/gcis_document/201911/4286628-11act8of2019criticalinfraprotectact.pdf> [Accessed 25 May 2022].

Smeets, M. & Achberger, B. 2022. Cyber hacktivists are busy undermining Putin's invasion. *The Washington Post*, 13 May. Available at: <https://www.washingtonpost.com/politics/2022/05/13/cyber-attack-hack-russia-putin-ukraine-belarus/> [Accessed 27 May 2022].

Smith, C. 2021. SA ports in crisis as Transnet cyberattack creates 'total nightmare' for exporters. *Fin24*, 28 July. Available at: <https://www.news24.com/fin24/companies/sa-ports-in-crisis-as-transnet-cyberattack-creates-total-nightmare-for-exporters-20210728> [Accessed 1 June 2022].

Snowden, N. 2021. *Triple extortion ransomware: A new challenge for defenders*. MORPHISEC. Available at: <https://blog.morphisec.com/triple-extortion-ransomware-a-new-challenge-for-defenders> [Accessed 10 June 2022].

SSA (State Security Agency). 2015. National Cybersecurity Policy Framework. *Government Gazette*, 39475. Available at: <https://www.gov.za/sites/default/files/gcis_document/201512/39475gon609.pdf> [Accessed 25 May 2022].

Sternstein, A. 2012. *Hackers manipulated railway computers, TSA memo says*. NextGov. Available at: <http://www.nextgov.com/cybersecurity/2012/01/hackers-manipulated-railway-computers-tsa-memo-says/50498/> [Accessed 27 May 2022].

Swanbeck, S. 2015. *Coast guard commandant addresses cybersecurity vulnerabilities on offshore oil rigs.* Center for Strategic and International Studies. Available at: <https://www.csis.org/blogs/strategic-technologies-blog/coast-guard-commandant-addresses-cybersecurity-vulnerabilities> [Accessed 27 May 2022].

Theoharidou, M., Kandias, M. & Gritzalis, D. 2011. Securing transportation-critical infrastructures: Trends and perspectives. In C.K. Georgiadis, H. Jahankhani, E. Pimenidis, R. Bashroush & A. Al-Nemrat (eds.). *Global security, safety and sustainability & e-democracy.* Lecture notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, Volume 99. Berlin: Springer, 171-178.

Toyana, M. 2021. Transnet cyberattack puts employees' salaries at risk while backlogs at ports mount. *Daily Maverick*, 26 July. Available at: <https://www.dailymaverick.co.za/article/2021-07-26-transnet-cyberattack-puts-employees-salaries-at-risk-while-backlogs-at-ports-mount/> [Accessed 28 July 2021].

Transnet. 2021a. *Annual results announcement for the year ended 31 March 2021*. Available at: <https://www.transnet.net/InvestorRelations/AR2021/2021%20ANNUAL%20RESULTS%20PRESENTATION.pdf> [Accessed 24 May 2022].

Transnet. 2021b. *Transnet Freight Rail 2021.* Available at: <https://www.transnet.net/InvestorRelations/AR2021/Transnet%20Freight%20Rail.pdf> [Accessed 24 May 2022].

Transnet. 2021c. *Transnet Pipelines 2021*. Available at: <https://www.transnet.net/InvestorRelations/AR2021/Pipelines%202021.pdf> [Accessed 24 May 2022].

Transnet National Port Authority. 2010. *Transnet National Port Authority*. Available at: <https://www.transnetnationalportsauthority.net/> [Accessed 3 June 2022].

Transnet Port Terminals. 2013a. *Commodity overview*. Available at: <https://www.transnetportterminals.net/Commodities/Pages/default.aspx> [Accessed 20 May 2022].

Transnet Port Terminals. 2013b. *ICT at Transnet Port Terminals*. Available at: <https://www.transnetportterminals.net/About/Pages/ICT.aspx> [Accessed 20 May 2022].

Transnet Port Terminals. 2013c. *Navis Sparcs N4*. Available at: <https://www.transnetportterminals.net/About/Pages/Navis.aspx> [Accessed 20 May 2022].

TSA (Transportation Security Agency). 2022. *Surface Transportation Cybersecurity Toolkit*. Available at: <https://www.tsa.gov/for-industry/surface-transportation-cybersecurity-toolkit> [Accessed 15 June 2022].

UNCTAD (United Nations Conference on Trade and Development). 2018. *Maritime trade and Africa*. Available at: <https://unctad.org/press-material/maritime-trade-and-africa> [Accessed 17 May 2022].

UNCTAD (United Nations Conference on Trade and Development). 2021. Review of Maritime Transport 2021. Available at: https://unctad.org/publication/review-maritime-transport-2021> [Accessed 30 November 2023].

USGS (United States Geological Survey). 2020. *Mineral commodity summaries 2020*. Available at: <https://pubs.usgs.gov/periodicals/mcs2020/mcs2020.pdf> [Accessed 31 May 2022].

Van Niekerk, B. 2017. Analysis of cyber-attacks against the transportation sector. In M.E. Korstanje (ed.). *Threat mitigation and detection of cyber warfare and terrorism activities.* Hershey, PA: IGI-Global, 68–91.

Van Niekerk, B. & Ramluckan, T. 2019. Economic information warfare: Feasibility and legal considerations for cyber-operations targeting commodity value chains. *Journal of Information Warfare*, 18(2), 31–48.

Wagstaff, J. 2014. All at sea: Global shipping fleet exposed to hacking threat. *Reuters*, 24 April. Available at: <https://www.reuters.com/article/us-cybersecurity-shipping-idUSBREA3M20820140424> [Accessed 27 May 2022].

Ware, W.H. 1998. *The cyber posture of the national information infrastructure*. Santa Monica, CA: RAND Institute.

Warrick, J. & Nakashima, E. 2020. Officials: Israel linked to a disruptive cyberattack on Iranian port facility. *The Washington Post*, 18 May. Available at: <https://www.washingtonpost.com/national-security/officials-israel-linked-to-a-disruptive-cyberattack-on-iranian-port-facility/2020/05/18/9d1da866-9942-11ea-89fd-28fb313d1886_story.html> [Accessed 27 May 2022].

Zetter, K. 2014. *Countdown to Zero Day: Stuxnet and the launch of the world's first digital weapon*. New York, NY: Crown.

Zukowski, D. 2022. Rail transit vulnerable to cyberattacks, experts say. *Cybersecurity Dive*, 23 February. Available at: <https://www.cybersecuritydive.com/news/rail-transit-cyberattacks/619123/> [Accessed 2 June 2022].