SOUTH AFRICA'S PORTS, PIPELINES AND HOSPITAL NETWORKS ARE CRITICAL INFRASTRUCTURE: PROTECTING THEM FROM CYBERATTACKS IS NON-NEGOTIABLE

Category: Privacy Law, Infosec, and POPIA,Technology Law
written by Lucien Pierce | August 4, 2021

MAERSK AND TRANSNET CYBERATTACK PARALLELS

On 27 June 2017, shipping company – Maersk – faced its biggest crisis. NotPetya, a type of ransomware, had spread through its global computer network in 7 minutes[1], destroying 49,000 of its laptop computers.[2] 17 of its terminals across the globe were hacked.

The NotPetya attack was so rapid, that at the Maersk terminal in Rotterdam, Netherlands, containers that were being transferred, simply stopped in mid-air.[3] Maersk was only able to resume online bookings after 10 days. The attack cost Maersk between US$300-350 million.

South African state-owned port, rail and pipeline operator – Transnet – appears to have suffered a similar fate. On 22 July it suffered what it initially called "*a disruption on its IT network*", later calling it a "cyberattack". Thankfully, its network appeared to have come back online by Monday 2 August.

What is significant about this particular incident is that it follows a number of recent major critical infrastructure-related cyberattacks. The most significant is probably the Colonial Pipeline hack. This incident required it to shut down its 8,850-kilometre pipeline, stopping the flow of up to 3 million barrels of fuel per day from its Houston facilities to the South-Eastern United States.

In Transnet's case, we do not yet know what the reason for the disruption was. News reports have been more explicit, calling it a "cyber-attack". If it was indeed a cyberattack, then this is going to be one of many more cyberattacks on South Africa's critical infrastructure. As we see from the examples below, critical infrastructure is more than just the country's road networks or power stations.

HOSPITALS, ELECTION SYSTEMS AND NATIONAL PAYMENT SYSTEMS INFRASTRUCTURE

If we think the recent unrest in KwaZulu-Natal and Gauteng disrupted the South African government's Covid-19 vaccination programme in those provinces, imagine the country-wide disruption that will occur if a cyberattack disrupts the Covid-19 Electronic Vaccination Data System (EVDS). This is certainly possible: the UK's National Health Service, hospital networks in the United States and Ukraine lost access to medical records because of cyberattacks. In Ukraine, the system that tracked one hospital network's ambulances, using GPS, was disrupted delaying response times to get to patients.[4] These are all incidents that likely had life-threatening consequences.

Consider the consequences of the Independent Electoral Commission's (IEC) Online Voter Registration Service or the Voters' Roll being compromised in a cyberattack. Even if no significant long-term harm happened to either, the reputational harm and damage to the integrity of the process, could fuel conspiracies, violence, dissent and even insurrection, much like we saw earlier this month. Again, this is not something theoretical or imagined. Former United States President Donald Trump is contesting the 2020 US presidential elections,[5] arguing that the voting system was compromised[6] or that Italian defence contractor's hackers had manipulated the US election.[7] Spurious as this may be, it rallied his supporters, resulting in the 6 January 2021 attacks on the US Capitol.

Think of the consequences of South Africa's National Payments System being compromised or perhaps the South African Social Security Agency's grants payment system.[8] This is not as far-fetched as you may think. When NotPetya spread across the world in 2017, Ukraine was particularly hard hit. One of its three critical (systemically important) banks, ATMs and its card payment systems were affected.[9] With high levels of poverty and dire circumstances, exacerbated by the inability to withdraw funds from banks, the consequences of a cyberattack, could well result in a repeat of the looting and lawlessness experienced earlier this month.

If the government wants to significantly reduce critical infrastructure cyberattacks, and the resultant economic damage, it must focus on, and make use of, those solutions and tools that are available, but which it is simply not using.

LAWS TO PROTECT CRITICAL INFRASTRUCTURE

We have a law, called the Critical Infrastructure Protection Act. It was enacted precisely to prevent incidents such as those that affected Transnet. This Act is intended to "*provide for measures to be put in place for the protection, safeguarding and resilience of critical infrastructure*." There is no doubt that institutions like Transnet, the IEC, the EVDS and the National Payments System are critical infrastructures. This is because the Act regards critical infrastructure as anything whose functioning is essential to the economy, national security, public safety and the continuous provision of basic public services, and whose loss or disruption may severely prejudice the State's functioning or public interest. But, this Act, which sets out how critical infrastructure must be protected, and became law in 2019, is not effective yet: even with all the critical infrastructure cyberattacks that we have seen in recent times.

We have another law – the Cybercrimes Act – which was enacted to deal specifically with the types of cyberattacks that Transnet is likely to have suffered. It is intended to make it easier for investigating agencies to obtain evidence and to seek assistance from similar agencies in other countries. It would allow for the easier prosecution of incitement that occurs through social media. It compels the Minister of Police to "*ensure that members of the South African Police Service receive basic training in aspects relating to the detection, prevention and investigation of cybercrimes*" and work with higher learning institutions to "*develop and implement accredited training programmes for members of the South African Police Service primarily involved with the detection, prevention and investigation of cybercrimes*". But again, much like the Critical Infrastructure Protection Act, this law is also not yet effective.

As a nation that wants to be at the forefront of the information age and as we become more reliant on information technology to operate critical infrastructure like ports, railways, pipelines, hospital networks and election systems, we need to recognise the significant harm cyberattacks can cause to our democracy and economy. When, not if, more damaging cyberattacks occur, because they certainly will, we need to be prepared and not "shocked" or "caught with our pants down", as has become the refrain in recent times.

[1] Maersk Notpetya Crisis Response Case Study (slideshare.net)

[2] https://www.securityweek.com/maersk-reinstalled-50000-computers-after-notpetya-attack

[3] The Maritime Industry's Move to Automation: Will This Make It a Hacker's Playland? | Institute of World Politics (cyberintelligence.world)

[4] https://www.avast.com/c-eternalblue

[5] https://campaignlegal.org/update/compiling-truth-resource-refute-trumps-stolen-election-lies

[6] https://www.cisa.gov/news/2020/11/12/joint-statement-elections-infrastructure-government-coordinating-council-election

[7] https://www.washingtonpost.com/investigations/italygate-michele-edwards-meadows-trump/2021/06/19/2f6314d2-d05f-11eb-8014-2f3926ca24d9_story.html

[8] SARB – National Payments System

[9] https://thehill.com/opinion/national-security/565173-capitol-insurrection-hearing-exposes-trumpworld-delusions