

South Africa needs stronger security in place to stop the sabotage of its power supply

By [Sascha-Dominik \(Dov\) Bachmann](#) and [Dries Putter](#)

4 Aug 2022

South African president Cyril Ramaphosa recently [outlined](#) plans to solve the country's devastating electricity supply crisis. But he didn't mention the country's ability to protect its energy infrastructure as a prerequisite to any solution.



Source: Mike Hutchings/Reuters

South Africa has had power cuts [since 2007](#) when Eskom, the power utility, began failing to meet demand. This got worse every year. The power utility is struggling to keep its [aged coal-fired power stations](#) running after many years of poor maintenance. It is also [struggling](#) to get its two new power stations to operate at full capacity.

Explaining some of the recent power cuts, Ramaphosa said that some of the energy infrastructure had been [sabotaged](#).

We flagged this in an earlier [article](#). We argued that Eskom was the target of hybrid warfare operations aimed at destabilising South Africa's national power generation capability.

The question is whether the country has the necessary security capabilities to protect its energy infrastructure from such threats and risks. An assessment of the security capabilities also has to include a fit-for-purpose test of the legislation for the [protection of critical infrastructure](#).

Enhanced intelligence capacities are required to detect, deter and neutralise threats such as sabotage, or subversion caused by rioting. More – and appropriately equipped – security forces are also needed to physically secure critical infrastructure. These could be privately or publicly funded.

Our view is that the country does not have what is required where and when it is needed. A comprehensive approach is needed – including managing security threats – to address its energy crisis. This requires collaboration between the state and private sector to implement the president's long-term energy security vision.



Government to take on Eskom debt, but unclear how much

Alexander Winning and Bhargav Acharya 2 Aug 2022



Hybrid attacks now common

South Africa is not the only country whose energy infrastructure is facing security threats. There are [numerous examples](#) of attacks on critical infrastructure. These are typically [cyber-related](#). But physical attacks such as [sabotage](#) also occur.

The [Institute for Security Studies](#) argues that attacks on the critical infrastructure of developing countries, such as South Africa, could be “[potentially devastating](#)”. South Africa’s national security vulnerabilities, combined with the security risks to a monolithic state-owned entity with no backup, could exacerbate the country’s power supply insecurities.

Cyber attacks on Eskom’s critical infrastructure could lead to severe damage. The result could be corresponding losses of generation capacity and damage to the economy.

National security vulnerabilities can be reduced by state security capabilities that are equal to the task. A [Report of the Expert Panel](#) into [civil unrest](#) in the country in July 2021 revealed serious capacity problems within the state security sector. The sector is mandated to forewarn government, and to protect critical infrastructure and the public against [hybrid threats](#). These include terrorism, subversion, sabotage, espionage and organised crime.

This weakness was also highlighted in the 2018 [High-Level Review Panel on the State Security Agency](#). It concluded that the country’s [State Security Agency](#) had been

“*compromised by factionalism, mismanagement and inefficiency.*”

The agency is South Africa’s primary authority tasked with protecting the country against such hybrid threats. Yet it is in a state of disrepair. This calls for the country to focus efforts on (at least) the capability to secure Eskom against obvious national security threats.



Eskom appoints two contractors for BESS initiative

1 Aug 2022



The importance of critical infrastructure

The protection of South Africa’s energy infrastructure falls within the remit of the new [Critical Infrastructure Protection Act 8 of 2019](#). Such infrastructure is crucial for the effective functioning of the economy, [national security](#) and public safety.

Critical infrastructure consists of national assets that are viewed as having strategic importance. South Africa has plenty of critical infrastructure spread across its length and breadth – measuring [about 1.219 million km²](#). These include the Eskom energy grid – [including power stations, sub-stations and transmission networks](#) – dams, the banking system and oil storage. The sheer scale requires extensive security capabilities necessary for physical protection and monitoring threats.

Beyond physically securing this infrastructure, the state also needs to have the ability to detect, deter and neutralise threat actors. These are classical counterintelligence prerogatives. Failure on this front makes the country vulnerable to destabilisation.

The [stretched nature](#) of the country's security agencies was laid bare during the [violent riots](#) in July 2021. It is thus reasonable to question the capacity of the police, and other security agencies, to secure Eskom's critical infrastructure and that of private power producers.



Eskom in talks with Botswana about importing power

28 Jul 2022



Planning for security

In our view, all planning to develop and diversify the national power grid and energy supply should include enough resources to protect them. This requires cooperative planning between Eskom and the South African security sector (both state and private).

The exact role of the South African National Defence Force in providing security for critical infrastructure remains unclear. The [National Key Points Act 1980](#), the [Defence Act 2002](#) and the [Critical Infrastructure Protection Act 8 of 2019](#) are not explicit on the issue.

The protection of critical infrastructure has been assigned to the South African Police Service, with the defence force [supporting it](#). Given that the defence budget has been shrinking annually, the military will probably not be able to sustain this.

With the private sector playing an increased role in the energy sector, South Africa needs to develop dedicated private security capacities to protect its critical infrastructure. At the very least, it should adopt a mixed public-private security model akin to the police service's [community policing](#) concept.

The president's energy vision envisages a much larger private industrial capacity. If left unsecured, such capacity would be just as vulnerable to sabotage as the current Eskom infrastructure is. It is time the country took stock of its security requirements in the same way it has started being serious about its energy vulnerabilities.

There's also the question of whether the penalties prescribed by law are fit to deter sabotage.

What needs to happen

The hybrid nature of [threats to the country's infrastructure](#) can only be solved by an integrated solution. That requires, firstly, clarity about mandates as well as state security capabilities.

Secondly, security sector capacity needs to be developed alongside critical infrastructure. Thirdly, legislation needs to

increase existing sanctions in terms of fines and imprisonment.

Lastly, public-private security partnerships must be established to bolster the security of the country's electricity infrastructure.

This article is republished from [The Conversation](#) under a Creative Commons license. Read the [original article](#).

ABOUT THE AUTHOR

Sascha-Dominik (Dov) Bachmann, professor in law and co-convener, National Security Hub, University of Canberra. Dries Rutter, lecturer at the Faculty of Military Science, affiliate member, National Security Hub, University of Canberra, and researcher for Security Institute for Governance and Leadership in Africa (SIGLA), Stellenbosch University.

For more, visit: <https://www.bizcommunity.com>