IPPR

BY **FREDERICO LINKS**

JUNE 2024

PROBLEMATIC INFLUENCES: African national security narratives impacting Namibian cybersecurity and cybercrime law-making

CIPESA

This work was carried out in the context of the Africa Digital Rights Fund with support from the Collaboration on International ICT Policy for East and Southern Africa (CIPESA).

1. What is the problem?

National security in many African contexts has become something of a magical incantation through which states can inflict anything, make anything disappear or keep anything hidden.

It goes without argument that a state's mandate to protect national security is a legitimate one and that the state should have the primary role in protecting national security.

However, globally national security has increasingly become a very problematic framing of state approaches to cyberspace and digital technology law and regulation crafting and enforcement.

This is because in many countries around the world the state increasingly invokes the mantra of national security to enable authoritarian repressions and human rights violations. Concerning cyberspace and digital technologies, these repressions and violations have primarily been perpetrated via cybersecurity and cybercrime related laws and enforcement mechanisms.

In May 2019 the UN Special Rapporteur on the rights to freedom of peaceful assembly and of association noted in this regard: *"A surge in legislation and policies aimed at combating cybercrime has also opened the door to punishing and surveilling activists and protesters in many countries around the world. While the role that technology can play in promoting terrorism, inciting violence and manipulating elections is a genuine and serious global concern, such threats are often used as a pretext to push back against the new digital civil society."*

National security in many African contexts has become something of a magical incantation through which states can inflict anything, make anything disappear or keep anything hidden.

National security is in many African contexts invoked primarily and narrowly in the interests of regime security and not all-of-society or human security. As a consequence of this warped framing, many Africans remain vulnerable to actual cyberthreats, abuses and crimes.

Regarding this, Privacy International has noted: *"When Governments argue for security they often focus on criminalising and monitoring online behaviour through repressive cyber crime laws and increasing state surveillance powers rather than addressing the root problem of insecure systems. Companies and governments build systems, devices, networks and services that accumulate vast data stored without proper regard to risk, security, or data minimisation. All of these approaches ultimately make people and their data less secure, and violate human rights."*

With specific reference to African states' actions, in its 2019 State of Internet Freedom in Africa report, the Collaboration on International ICT Policy for East and Southern Africa (CIPESA) concluded: *"The implementation of oppressive laws and regulations is on the rise in the countries under review. It is evident that countries are using legislation to legitimise practices which are otherwise unlawful to impose restrictions and internet controls. While laws in place are touted as necessary towards fighting cybercrime or enhancing cybersecurity in the countries [under review], they are largely directed towards stemming opposition, clamping down on criticism and quelling local dissent."*

2. Why have national security framings and narratives become so problematic?

> *It appears that leaders continue to enact legislation and implement measures to safeguard their selfish political interests, sometimes clothed as legitimate public interests.*
>
> — CIPESA, 2019

In the African context, national security narratives around cyber and digital technology law and regulation have become problematic because it is clear that these narratives are about increasing state control measures and mechanisms over online and digital spaces.

And as CIPESA noted in 2019: *"These controls collectively continue to undermine democracy and cement authoritarians' hold on political power. Political censorship continues to be used to block perceived offensive content in order to maintain the status quo and remain in power. Such measures have been more rampant during election periods and they include propagating set narratives, limiting the spread of information by their competitors, and blocking information that does not favour their positions. It appears that leaders continue to enact legislation and implement measures to safeguard their selfish political interests, sometimes clothed as legitimate public interests."*

To be clear, this suggests that African states on the whole can arguably be labelled as largely being national security states, in that there has been a demonstrated tendency to frame just about every socio-economic and political issue across countries as a national security consideration.

Against this backdrop, in order to achieve a measure of near total control over online and digital spaces, many African states, including Namibia, are continuously expanding the mandates of state security agencies and the issues that can be classed as national security issues. In order to do this, highly problematic laws are increasingly being drafted and enacted to combat such issues as online hate speech or disinformation, but that are then also used to suppress free expression or to justify such state actions as internet shutdowns. In most cases, state security actors then also make telecommunications and internet service providers complicit in all sorts of violations.

This concerning trend of widening national security mandates and lumping of issues into the national security basket, and the compromising of telecommunications and internet service providers, led to former UN Special Rapporteur on free expression, David Kaye, to state in 2018: *"Broadly worded restrictive laws on "extremism", blasphemy, defamation, "offensive" speech, "false news" and "propaganda" often serve as pretexts for demanding that telecommunications companies suppress legitimate discourse."*

It should be noted though that in Africa, insecurity and instability are probably largely caused or significantly contributed to by state failings or actions. Very often, African states or state actors are the primary violators of human rights and drivers of extremism, or the primary perpetrators of "false news" and "propaganda", but unsurprisingly these actors never articulate their own actions, or lack thereof, as national security threats.

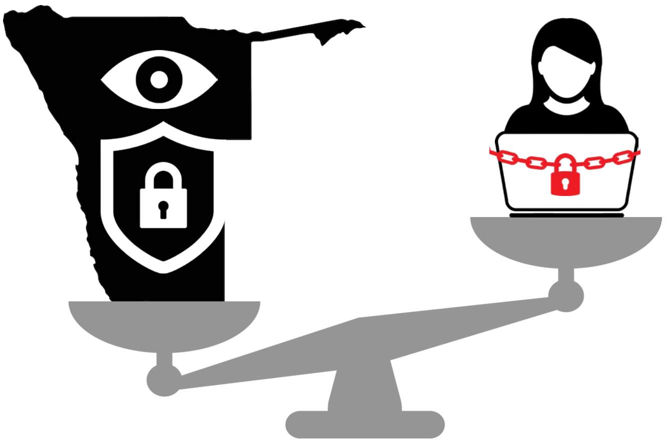
3. What are the problematic narratives?

There are specific African state national security narratives that have now become evident and problematic in Namibian government approaches to cybersecurity and cybercrime law-making.

These narratives can be grouped under the following descriptors (in no particular order):

- State information security;
- Security outweighs privacy;
- Mass surveillance is necessary;
- Radicalisation and terrorism;
- The nothing-to-hide argument.

These narratives link to and reinforce each other, as the following discussions show.

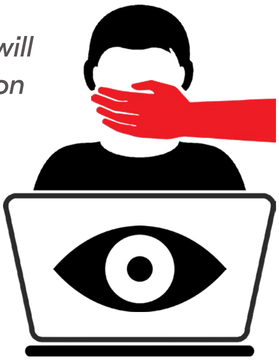


3.1 State Information security

The narrative that is promoted is one that couches state information security as an overriding national security priority.

African state cultures, to varying degrees, prize secrecy and confidentiality over openness and transparency. In this sort of culture, access to information and those demanding it are considered security threats. The implicated mindset is one that considers maintaining a firm security grip on information in the state's possession a national security priority and views the very existence of such information as a security threat. This sort of reasoning has also been evident in Namibian government approaches to the issue of information security in the cyber context.

This can mean that any information in the possession of the state can be labelled as secret, effectively ensuring that media freedom becomes a related national security issue. This enables states to limit the media and journalists in any way possible, even doing so outside the law or using any legal measure available, as indicated by a 2023 study of the impacts of Southern African Development Community (SADC) cybercrime laws on media freedom.



The study found that: *"Where there is political will to inhibit speech, legal tools will be found. Some SADC countries have used mechanisms as unexpected as aviation regulations, allegations of non-payment of utility accounts and bogus charges of illegal drug trafficking to harass journalists and shut down media businesses."*

The prioritising of state information security as a national security objective does not recognise that cybersecurity is about *"protecting and defending individuals, devices and networks"*, even from state access and scrutiny, as Privacy International and others argue.

3.2 Security outweighs privacy

> *In this current age of global insecurity, governments and their spy agencies keep telling us that we need to live with increasingly invasive state spying for our own sakes.*

Another problematic narrative influencing Namibian cybersecurity and cybercrime law and policy discussions is the one that proposes that security considerations trump human rights considerations.

The narrative that many Africans across the continent have had to come to terms with over the years is one that forces them to accept that they have to basically give up their right to communications and online privacy in exchange for safety and security.

Jane Duncan, in her 2022 book 'National Security Surveillance in Southern Africa: An Anti-Capitalist Perspective', articulates this state-driven national security position and its pitfalls quite clearly: *"In this current age of global insecurity, governments and their spy agencies keep telling us that we need to live with increasingly invasive state spying for our own sakes. Bulk, dragnet surveillance, we are told, is a necessary evil, and we must be prepared to give up some rights to become safer. Yet, there is a disturbing pattern the world over in how national security surveillance agencies conduct themselves. They claim more and more power and bigger budgets on national security grounds, yet we never seem to become any safer. Repeatedly, they are exposed as having abused their powers, where the supposed protectors of national security become the very people who threaten it. Scandals about intelligence agencies spying on journalists, academics, civil society and opposition political parties have become frequent occurrences. In fact, we have become used to the spies sticking their noses where they do not belong, while not sticking their noses where they do belong. When the spies are exposed for abusing their powers and the public trust, it has become all too easy for them to blame rogue elements and commit to cleaning up their acts. Until the next time."*

3.3 Mass surveillance is necessary

The security-outweighs-privacy narrative goes hand-in-hand with the one that encourages Namibians to normalise mass surveillance, through such measures as mandatory SIM card registration and mandatory data retention. These measures are now to be found in basically all African states.

With regard to mandatory SIM card registration, Jane Duncan states: *"Mandatory SIM card registration is a form of mass surveillance, as it involves the indiscriminate collection and storage of personal details when a SIM card is registered in an individual's name, and mobile phone users who opt out of the registration process do so on pain of being disconnected from the network. The effect of SIM card registration is that users cannot communicate anonymously without the potential for being tracked."*

African states promote mandatory SIM card registration, and data retention, as national security imperatives for enhancing and maintaining cybersecurity and countering mobile phone-based cybercrime. However, the evidence of this effectiveness is questionable at best.

In 2019, Privacy International stated that *"while governments justify mandatory SIM card registration laws on the grounds that they assist in preventing and detecting crime, "there is no convincing empirical evidence that mandatory registration in fact systematically lowers crime rates,"* and *"no robust empirical studies that show that such measures make a difference in terms of crime detection"*.

This is echoed by Duncan, who points out that: *"SIM card registration is notoriously ineffective as a crime-fighting tool, as criminals are more likely to use creative workarounds to prevent themselves from being tracked (such as buying pre-registered SIM cards that are sold illegally)."*

3.4 Radicalisation and terrorism

The expansion of the national security mandates and practices of state security agencies across the continent is justified by national security states in pointing to what they perceive to be rising radicalisation and threats of terrorism. However, in most instances these threats are significantly overblown, as legitimate political expression and protests are often also framed in terms of radicalisation and terrorist threats to the state.

In 2021, CIPESA noted that state surveillance *"is increasingly being used by various African governments to entrench political control, including through targeted profiling and spying on activists, human rights defenders, journalists, opposition leaders, and political dissidents perceived to be critical of the ruling administrations"*.

CIPESA goes on to state: *"The continued rise in surveillance cannot be divorced from the growing affronts to digital civic space in the region. State surveillance is a key component of wider efforts by a significant number of African governments deployed in an ever-expanding raft of measures to undermine and clamp down on their citizens' ability to openly and freely use digital technologies. Such control measures are specifically aimed at curtailing expression and organising that is critical of governments and state officials."*

Since the Arab Spring of the early 2010s, youth activism across the continent has especially become a focus of the African state's national security gaze. In Namibia, the intelligence service has also pointed to alleged youth radicalisation and terrorism (which is not an issue for the country) as reasons to increase its digital surveillance operations.

3.5 The nothing-to-hide argument

Another highly problematic narrative that Namibians have to contend with regularly when speaking out against the invasive digital surveillance practices of the Namibian national security state is the nothing-to-hide argument — basically, if you have nothing to hide, then you have nothing to fear, so why make an issue of state surveillance and the undermining of digital rights. This is an argument that has been used by many other African governments over the years. The implied question that is posed to anybody opposing state practices such as mandatory SIM card registration is, of course, whether they are afraid of being exposed. Once again, this is an encouragement to normalise state mass surveillance and to willingly accept the limiting of fundamental human rights.

While most Africans probably have little to hide, African states on the other hand have much to obscure. For it is true that the national security-related violations and abuses of African states are increasingly well-documented. In this regard, CIPESA noted in 2021: *"Government critics including leading opposition leaders, human rights defenders and activists who do human rights and governance work, as well as investigative journalists, are prominent targets of state surveillance. The stated reasons for conducting surveillance are to ensure national security and tackle terrorism, cybercrime, riots, hate speech and violence. However, as the study shows, state surveillance primarily targets political opponents, dissidents and critics, human rights defenders, activists and journalists simply because of their work. This indeed supports a key finding of the study that, one of the objectives of surveillance in the region is to enable the state to perpetuate censorship by silencing or stifling criticism especially about state accountability and corruption."*

4. How are these narratives playing out in Namibia?

As has been illustrated, Namibian state authorities are using the same narratives, to greater or lesser degrees, that other African states have deployed and that have become problematic across the continent. Not only that, since April 2024 mass state surveillance has also become a reality in Namibia as the country has implemented mandatory SIM card registration and data retention against the narrative backdrop of national security.

5. What can be done about this?

While the power imbalance between the state and civil society, and the news media, is a real concern, it nevertheless remains the case that Namibian civil society and news media need to counter state national security narratives that could enable human rights violations, both online and offline, limit the emergence of robust online civic spaces, and undermine digital democracy.

Targeted policy advocacy and sustained activism around the issues raised in this report should be considered as viable to spread information about the state's problematic national security narratives and framings in the context of cyberspace and digital technology law and regulation crafting and enforcement.

About the Author

Frederico Links is a Namibian journalist, researcher and freedom of expression advocate. As a researcher he is affiliated with Namibia's leading independent think-tank, the Institute for Public Policy Research (IPPR), where he coordinates a number of projects. In both his journalism and research, Links has a strong focus on good governance, human rights (including digital rights), corruption, rule of law, and transparency and accountability.

About CIPESA

The Collaboration on International ICT Policy for East and Southern Africa (CIPESA) is one of two centres established under the Catalysing Access to Information and Communications Technologies in Africa (CATIA) initiative, which was funded by the UK's Department for International Development (DfID). CIPESA focuses on decision-making that facilitates the use of ICT in support of good governance, human rights and livelihoods.

CIPESA's establishment in 2004 was in response to the findings of the Louder Voices Report for DFiD, which cited the lack of easy, affordable and timely access to information about ICT related issues and processes as a key barrier to effective and inclusive ICT policy making in Africa. As such, CIPESA's work responds to shortages of information, resources and actors consistently working at the nexus of technology, human rights and society.

https://cipesa.org/

About the IPPR

The Institute for Public Policy Research (IPPR) is a not-for-profit organisation with a mission to deliver independent, analytical, critical yet constructive research into social, political and economic issues that affect development in Namibia. The IPPR was established in the belief that free and critical debate informed by quality research promotes development.

Institute for Public Policy Research (IPPR)
House of Democracy
70-72 Frans Indongo Street
PO Box 6566 Windhoek
Namibia
info@ippr.org.na
www.ippr.org.na
Tel: +264 61 240514