DEMOCRACY REPORT

BY FREDERICO LINKS | Special Briefing No. 28 | JUNE 2019

Democracy Report is a regular publication featuring analysis and commentary relating to the legislative agenda of the Parliament of the Republic of Namibia. It is produced by the Institute for Public Policy Research (IPPR), PO Box 6566, Windhoek, Namibia. Tel: +264 61 240514, Fax: +264 61 240516,info@ippr.org.na. The publication is also available as a PDF download from http://www.ippr.org.na. Democracy Report is funded by the Embassy of Finland

Embassy of Finland
Windhoek

KEY OBSERVATIONS AND RECOMMENDATIONS

Key observations

Evidence indicates that Namibia has acquired sophisticated communications interception and surveillance capabilities, that those capabilities have been deployed, and that the deployment of these capabilities is legally questionable.

This is because the legal framework enabling communications monitoring, interception and surveillance – Part 6 of the Communications Act of 2009 – has not been brought into force yet, by the Namibian government's own account.

Thus, it can plausibly be argued, communications interception and surveillance overreach and abuse characterise whatever interception and surveillance activities and practices are being carried out by state security and intelligence services.

This presents a challenge and a threat to the rule of law, Namibia's constitutional order – as the right to privacy is constitutionally enshrined – and ultimately to a still emergent democracy. Unchecked surveillance, if suspicions about such activities and practices are prevalent enough in society, has a 'chilling effect' on freedom of expression and association and could potentially lead to widespread self-censorship and a silencing of legitimate political expression.

RECOMMENDATIONS

Against this backdrop, the following recommendations are made:

1. That relevant Namibian government authorities urgently clarify the implementation status of Part 6 of the Communications Act of 2009;
2. That relevant Namibian government authorities review and amend the clauses of Part 6 of the Communications Act of 2009 to make provision for or improve public oversight mechanisms and abuse-mitigating safeguards in the communications interception and surveillance practices of the Namibia Central Intelligence Service (NCIS), as well as doing away with discretionary powers and non-accountable operations;
3. That, in general, more transparency is introduced into the workings and practices of state security, intelligence and law enforcement agencies and their functions that concern communications monitoring, interception and surveillance;
4. That specifically strengthening judicial and parliamentary oversight, as well as incorporating some form of independent oversight, be part of improved transparency mechanisms aimed at installing workable checks and balances into the frameworks governing the activities of state security and intelligence services and operatives;
5. That measures to reform communications interception and surveillance practices be guided by the 13 'International Principles on the Application of Human Rights to Communications Surveillance';
6. That relevant Namibian authorities move to draft and enact a comprehensive data protection and privacy legislative and regulatory framework;
7. And, similarly, that relevant Namibian authorities move to finalise the drafting and enactment of an access to information law which would aid the public, civil society and the media, as well as other stakeholders, in ensuring various strategic state actors are held accountable for their actions, including those involved in communications monitoring, interception and surveillance.

1. 'WE ARE LIVING IN THE AGE OF SURVEILLANCE'[1]

Surveillance by both states and private actors has increasingly become a political threat over the course of the second decade of the 21st century. As this decade draws to a close, surveillance has become one of the major factors said to be undermining human rights around the world; especially in emerging democracies like Namibia.

Of significant concern is the issue of state communications monitoring, surveillance and interception, as the use of sophisticated surveillance technologies has spread around the world and as states increasingly use such technologies to spy on citizens – often on journalists and human rights and democracy activists. In many of these instances such surveillance practices appear to be extrajudicial or unconstitutional.

The global situation has become so worrying that UN Special Rapporteur on the Right to Privacy, Joseph Cannataci, stated in a surveillance and privacy report[2] in February 2018 that: "The issue of surveillance is an extremely sensitive one. Some experts have described the current situation in the area as one where most states have either resisted legalisation or have been ambivalent about prioritising rights where national security threats are politically resonant. There is a significant concern that states are far from ready to move in a rights-positive direction on surveillance, and that a draft legal instrument could indeed be an opportunity for regressive negotiation."

Cannataci goes on to say that states should be discouraged from legitimising and developing "questionable and bad" surveillance practices because such practices "ultimately weaken human rights, the national and international legal order and result in a situation which threatens to lower human dignity and cause physical harm to persons all over the world".

What the Cannataci statements ultimately point to is the general absence of appropriate oversight and adequate regulation of state security and intelligence agencies' communications monitoring, interception and surveillance capabilities and practices the world over, and how this general lack of oversight and regulation has fuelled suspicions of widespread surveillance abuse – suspicions stoked and largely confirmed by the Edward Snowden/NSA leaks of 2013.

Sadly, it would appear that Cannataci's warnings are both too late and too little, as abuse of communications surveillance capabilities has become disturbingly easy. For as Neil M. Richards states in his seminal 2013 paper on the dangers of surveillance: "The scope and variety of the types of surveillance that are possible today are unprecedented in human history. This fact alone should give us pause. But not only have the technologies of surveillance multiplied; so too have the entities that wish to surveil. Autocratic regimes have long been the villains in the stories we tell about surveillance, but they are no longer the only governments that have stepped up their surveillance activities."[3]

To underscore Richards' sentiments, with over half the world's population officially estimated to have connected to and regularly accessed the internet in 2018 and with mobile phones having become near ubiquitous, the potential for communications interception and surveillance and surveillance abuse have increased exponentially. In fact, with the global market penetration of internet-enabled mobile devices rising very fast, as the costs of such devices are decreasing all the time or as affordability has increased, such devices have become known as "the spy in your pocket".[4]

Because of this: "It is more than likely that the spies have been using mass surveillance (or surveillance that targets many people even if there isn't a reasonable suspicion of

1. Taken from Neil M. Richards, The Dangers of Surveillance, at: http://ssrn.com/abstract=2239412
2. Cannataci's Working Draft Legal Instrument on Government-led Surveillance and Privacy can be accessed at: https://www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/2018AnnualReportAppendix7.pdfhttps://www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/2018AnnualReportAppendix7.pdf
3. The Dangers of Surveillance can be accessed at: http://ssrn.com/abstract=2239412
4. This was initially the headline of a Time magazine article in 2006, that can be accessed with a subscription at: http://content.time.com/time/magazine/article/0,9171,1174705,00.html

criminality) and other powerful surveillance tools because they are so badly regulated," wrote University of Johannesburg media academic Jane Duncan in February 2018 in an article about surveillance abuse by South Africa's State Security Agency in the wake of numerous such abuse cases primarily involving the interception of the communications of journalists, democracy and anti-corruption activists and opposition leaders. These abusive surveillance practices have been numerously exposed by the media in that country over recent years.

Duncan states that spy agencies have traditionally argued that they needed wide-ranging powers of surveillance in order to forecast and anticipate threats to national security and in order to stay ahead of malevolent actors seeking to cause harm.

"But, spy agencies the world over are also being challenged over these arguments. In the wake of the Edward Snowden leaks which revealed how mass surveillance is being abused, increasingly people are not willing to take the spy agencies' arguments at face value," writes Duncan.

This provides an apt backdrop against which to situate this discussion, which is meant to be cautionary in tone and intent. For it is that there are also credible suspicions of and considerable circumstantial evidence for widespread communications surveillance abuse in the Namibian communications monitoring, interception and surveillance context.

This paper – through showing how Namibian state security and intelligence agencies have been procuring or attempting to procure surveillance technologies internationally – argues that state security agencies and authorities have been engaging in legally questionable and potentially unconstitutional surveillance practices and activities for most of the last decade, since about 2009, if not much earlier.

2. SECUROCRATIC CREEP AND NON-ACCOUNTABILITY

Any discussion of state surveillance – in the specific context of the abuse of such capabilities – needs to consider the political and legal environment and the security governance culture within which state security and intelligence authorities operate, as the nature of that environment and culture very much set the tone for how such authorities function.

The Economist Intelligence Unit's Democracy Index considers Namibia a flawed democracy[6] in which a single dominant party, the Swapo Party, has held near absolute power over a centralised government infrastructure since the dawn of the country's independence from apartheid South Africa in 1990, following a brutal and protracted war for independence of more than two decades.

In post-independence Namibia, allegiance to the ruling party has increasingly become a powerful currency, so much so that the lines between state and party have gradually blurred over the years since 1990. Party cadres and loyalists appear to have been appointed *en masse* to all levels of state. Consideration for the most senior posts in government in many cases appears to be determined primarily by party affiliation and liberation era credentials, rather than whether candidates or incumbents are best qualified, irrespective of their political affiliations. The hallmarks of a system of political patronage also appear visible in political appointments to certain senior positions within government.

The issue of party affiliation and liberation war credentials seems especially true in the military, law enforcement and intelligence sectors – the broad defence and safety and security establishment – where over the years command structures have largely been populated by former senior officers and commanders of Swapo's pre-independence People's Liberation Army of Namibia (PLAN) and its intelligence and security apparatus.

6. https://www.eiu.com/topic/democracy-index

Since independence in 1990, the Namibia Central Intelligence Service (NCIS) has had three directors-general – Peter 'Tshirumbu' Sheehama, Lucas Hangula and Philemon Malima – all of whom were PLAN commanders with links to Swapo's pre-independence security apparatus, as well as high-ranking members of the political inner-circle in post-independence Namibia.

This state of affairs has arguably enabled a governance culture characterised by secrecy, silence and impunity – especially in the state security and intelligence sector.

2.1 Securocratic creep

To appropriately situate the issues that follow, it should be understood that almost from the beginning, security-related narratives have come to underpin the formation of the Namibian state. 'Safety and security' concerns have underpinned calls for national reconciliation and unity, as well as social cohesion.

This subtle and incessant beating of the 'safety and security' drum is arguably a reflection of the continued power of securocratic elements within Swapo's upper echelons. During the liberation struggle, these elements were intensely preoccupied with internal security and enemy espionage and infiltration of party and military ranks from the 1970s through to 1989, when the war for liberation officially came to an end. In the process of ostensibly countering enemy espionage and infiltration – in a prolonged campaign that reportedly involved arbitrary arrests and detentions, torture, mutilation, and mass disappearances[7] – the organisation had itself built a formidable internal security and intelligence capability and apparatus. Historical and witness accounts paint a picture of a Soviet-style 'secret police' that wielded power with ruthlessness and impunity – much of which was transformed in the immediate post-independence period into the forerunner to what was eventually to become the Namibia Central Intelligence Service (NCIS) at the end of the 1990s.

To date there has been no accounting for the activities of the ruling party's pre-independence security apparatus, despite numerous and continued calls for commissions of inquiry or at least an official apology for the widespread human rights violations that took place in exile.

For as Leys and Saul pointed out in 2003, in the post-independence period many "find it difficult to accept that Namibia is truly 'new' so long as the commander of the armed forces is the alleged 'butcher of Lubango' and interrogators from the Lubango detention centres have been reincarnated as members of the Security Service or the President's Special Field Force, which has been involved in numerous reported instances of intimidation and harassment in recent years. In short, the feeling that the secret political culture of the Lubango detention centres has been dangerously carried forward, unexamined and unchecked, into independent Namibia, is not confined to the Lubango detainees and their families".[8]

"There is no room for doubt as to the seriousness of the indictment levelled against the Swapo leadership regarding its human rights abuses in exile. There is a wide range of recorded testimony," they wrote.

However, a thick cloak of secrecy has effectively been wrapped tightly around the official record of what Swapo security operatives did in the liberation era. This secrecy has been extended into the independent Namibia period, with the NCIS not being accountable to anyone other than the state president, as the agency operates out of the presidency, while parliament, as the body consisting of the supposed representatives of the people in a democracy, has very limited oversight over the agency, through the Standing Committee on Foreign Affairs, Defence and Security of the National Assembly.

7. For an account of such practices and first-hand experiences read Oiva Angula's Swapo Captive published by Penguin Random House South Africa (2018).
8. In 'Re-Examining Liberation in Namibia: Political Culture since Independence': https://www.questia.com/read/104610513/re-examining-liberation-in-namibia-political-culture

The committee's tasks include, amongst others, reviewing "the affairs and operations"[9] of the NCIS. However, the spy agency has apparently never submitted a report to the committee or made an appearance before it, which could point to lax oversight by the heavily Swapo-dominated committee. One media report stated that the committee did "not have access to any operational information of the agency and as such has not submitted a report to parliament".[10]

This centralisation of state security and intelligence gathering capabilities, and the discretionary power that comes with access to and control of such capabilities, can be argued to be contributory to a climate of abuse – taking the form of conduct, practices and activities outside the bounds of law and the constitution – towards achieving or maintaining narrow political and economic aims and interests – and even committing or hiding corruption – while proclaiming that such capabilities are being harnessed or deployed in the interest of 'national security', or not at all.

The issue of 'national security' is a significant point, for 'national security' has become something of a 'magical incantation', meant to convey that whatever it is tagged to is off limits to the public, and audaciously even any sort of regulatory or judicial oversight. It is under this tag that the abuse of the state's intelligence capabilities appears to be prevalent, as illustrated by recent and ongoing events, which will be discussed in the following section.

Image 1: The Patriot vs Spies cover

2.2 Abuse of power and secrecy

In 2018 the bright light of transparency was shone, arguably for the first time in a significant and sustained way, on the activities of the NCIS – in what were connected cases of alleged fraud and waste of state resources and grand corruption involving fishing quotas.

The first case involved the NCIS, and the Namibian government, unsuccessfully attempting to prevent the weekly *The Patriot* newspaper from publishing an article about "shady dealings"[11] at the spy agency involving the misuse of state assets. The spy agency used the apartheid-era Protection of Information Act [12] (Act 84 of 1982) in its attempted muzzling of the newspaper, claiming that the "publication of the information will jeopardise the national security".

Notably, during the court case it was revealed by the newspaper's editor that their investigations "into corruption allegations at NCIS have turned up information of absolute power which has made the spy agency non-accountable for tax payers' money".[13]

With regard to the issue of oversight, the newspaper reported in August 2018 that the "NCIS legal team is on record when it stated in the High Court that it wanted the spy agency to be insulated from both parliamentary and judicial oversight".

This was reported after the judge in the attempted muzzling case, Harald Geier, had ruled – in favour of *The Patriot* – in June 2018 that "the action of the NCIS is subject

9. http://repository.unam.na/bitstream/handle/11070/1482/Nauyoma2015.pdf?sequence=1&isAllowed=y
10. https://thepatriot.com.na/index.php/2018/08/17/fraud-rocks-ncis/
11. http://repository.unam.na/bitstream/handle/11070/1482/Nauyoma2015.pdf?sequence=1&isAllowed=y
12. https://thepatriot.com.na/index.php/2018/08/17/fraud-rocks-ncis/
13. https://thepatriot.com.na/index.php/2018/08/17/fraud-rocks-ncis/

to judicial oversight as it operates in the context of a democratic state founded on the rule of law which rules subjects, all public officials and all those exercising public functions, whether openly or covertly, in the interest of the State, to judicial scrutiny, this would include all operatives and functionaries of the NCIS".

The NCIS challenged the ruling in the Supreme Court, but in early April 2019 the court upheld the High Court judgement, with deputy chief justice Damaseb saying "the court did not agree with the government's argument that a court did not have the power to override the government and NCIS' designation of something as secret and a matter of national security. He stated: "The notion that matters of national security are beyond curial scrutiny is not consonant with the values of an open and democratic society based on the rule of law and legality".[14]

Image 2: Fraud rocks NCIS cover


Money fights rock NCCI | Page 3

The Patriot

Balanced and fair

17 AUGUST - 23 AUGUST 2018 | ISSUE 121

N$4.00

Fraud rocks NCIS

...'Incorruptible' spy agency's senior official in court for N$17m fraud

- 79 charges of fraud
- 79 charges of corruption

By Mathias Haufiku

A senior Namibian Central Intelligence Agency (NCIS) official appeared in the Windhoek Magistrate's Court on Wednesday for allegedly defrauding the spy agency of about N$17 million.

The 56-year-old official, whose name is known to The Patriot but cannot be revealed, appeared in camera after he was arrested by the Namibian Police in Ondangwa on Tuesday evening. The suspect was held at a secret location on Tuesday evening until he made his appearance at the Court on Wednesday morning.

It is understood that he faces 79 charges of fraud, money laundering, theft and corruptly using his office/position for gratification.

The official is one of the top five in the service's hierarchy.

Information at hand indicate that the official committed the heinous crimes between 2003 and 2011. The case was opened in 2013 with case no CR 216/10/2013. According to information available, the investigation is complete with the prosecution sanctioned by the Prosecutor General. It remains unclear why the arrest of the official took as long as five years given the seniority of the suspect.

His case was remanded to 18 October 2018 and he was released on bail of N$40 000. He will appear in the High Court.

His defence lawyer George Neves refused to comment when approached.

"This is a national security matter therefore I cannot comment. I am still waiting for disclosure because I have not seen the docket," said Neves.

In light of the high integrity required by officials in the agency, talks are rife that the accused could be suspended in due course.

This fraud case comes hot on the heels of a recent court loss for the NCIS when the High Court dismissed its application to block a news article which The Patriot intended to publish several shady deals it is involved in.

During the trial, the defence team of NCIS argued that the NCIS is incapable of committing any form of corruption and should thus not be subjected to judicial oversight.

TO PAGE 2

Philemon Malima

From the start the case was shrouded in secrecy, as "the presiding magistrate, Walter Mikiti, ordered that the official court record of the case, which would normally be a public record, be kept under wraps and not be made available to the media after a public prosecutor asked for such an order on the grounds of 'national security'".[16]

On this issue of blacking out information about the NCIS in court proceedings, Judge Geier had opined just two months earlier in the case around the attempted muzzling of *The Patriot* that "the provisions of the law [Protection of Information Act] can and should never be used for any illegal purpose or to cover up unlawful or potentially unlawful activity".

The corruption case of the senior NCIS official never went anywhere as the official died of suicide in September 2018, which meant the case was scrapped from the criminal court roll.

Another incident that bears mentioning in the context of the potentially illegal activities and the apparent considerable governance shortcoming at the NCIS was the March 2018 revelation that, despite having been effectively replaced in 2015, when Philemon Malima was appointed NCIS director-general, former director-general Lucas Hangula had simply refused to go and was at the time still receiving the full pay and

14. https://www.namibian.com.na/77625/read/Supreme-Court-affirms-judicial-oversight
15. https://www.namibian.com.na/181319/archive-read/Top-spy-found-dead
16. https://www.namibian.com.na/181319/archive-read/Top-spy-found-dead

benefits of a sitting director-general, as well as being in office.[17] Reports seemed to indicate that there were effectively two directors-general in office at the spy agency.

These are by no means the only reports of such instances of NCIS governance malfeasance, but what this section is meant to illustrate is that the intelligence service seems to be riven with corruption, mismanagement and the waste of state resources, and has abused the mantras of secrecy and 'national security' to cover up (or attempt to) illegal activities within its ranks and structures. These sorts of practices have arguably created an internal culture founded on the belief that the NCIS was not answerable to the courts or parliament (theoretically the public) and can operate outside the law.

This is one of the hallmarks of a hard securocratic mindset – a disregard of the rule of law when it suits – which seems to be a legacy of the pre-independence era when security and intelligence operatives, on both sides, were not held to account.

2.3 Key observations

- Namibia's political and legal environment have allowed a security and intelligence governance culture to emerge within state security and intelligence authorities that is a threat to the democratic order and the rule of law;
- This governance culture is characterised by secrecy, silence and impunity in the state security and intelligence sector;
- This culture, which is a holdover from the liberation era, seems to prize party affiliation and liberation era credentials in appointments – a process of cadre deployment which blurs the lines between party and state – to the senior ranks in the military, law enforcement and intelligence sectors;
- This contributes to discernible examples of corruption and mismanagement in the intelligence service, where the mantras of secrecy and 'national security' are used to cover up, or attempt to cover up, a number of legally questionable acts and practices;
- This is fuelled by and founded on the belief that state intelligence operatives are not answerable to the courts or parliament and **can and probably do** operate significantly outside the law;
- A notable concern is the fact that oversight mechanisms and safeguards against surveillance abuse and overreach are under-developed and weak, and that discretionary and non-accountable power rests within the presidency with regard to the deployment of state intelligence capabilities.

Who the 'enemies' are

Over recent years fears of 'radicalisation' or social unrest, or just the increasing assertive (and often offensive) outspokenness of youth, appear to have become concerns for national political and security leaders.

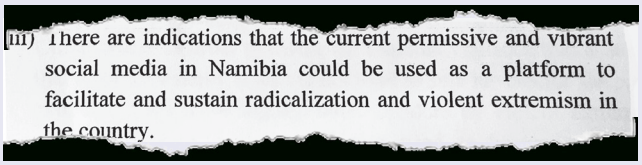
Namibia is not a politically unstable country wracked by territorial instability or violent extremism and insurrection. In fact, according to the Global Terrorism Index[18], Namibia consistently displays "no impact of terrorism", simply meaning that terrorism or violent extremism are not significant threats to the safety and security of the country as compared to other parts of the continent and the world.

However, in 2014 the Namibian parliament hastily – in the space of days – enacted the Prevention and Combating of Terrorist and Proliferation Activities Act, under which the Institute for Public Policy Research (IPPR) "warned that peaceful protesters, striking workers, social media users and journalists risk being charged under the anti-terrorism law that was rashly passed in the National Assembly".[19]

17. https://neweralive.na/posts/former-ncis-chief-refuses-to-go-venaani
18. http://visionofhumanity.org/app/uploads/2017/11/Global-Terrorism-Index-2017.pdf
19. https://www.namibian.com.na/print.php?id=139900&type=2

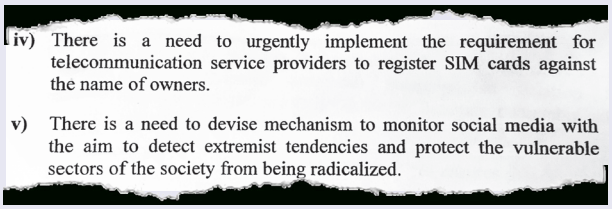
From 29-30 March 2017 a workshop was hosted by the Namibia Central Intelligence Service (NCIS), in collaboration with other government departments, on "preventing and countering of violent extremism", with the aim of "Enhancing National Security Through Collaborative Efforts". The workshop included participation by selected civil society organisations, including the IPPR.

Much of the content of the discussions at the workshop focused on youth radicalisation – over half the country's population is under the age of 35 – and amongst the assessments of the national situation was the following:


iii) There are indications that the current permissive and vibrant social media in Namibia could be used as a platform to facilitate and sustain radicalization and violent extremism in the country.

iii) There are indications that the current permissive and vibrant social media in Namibia could be used as a platform to facilitate and sustain radicalisation and violent extremism in the country.

At the end of the two-day workshop, amongst the recommendations were the following:

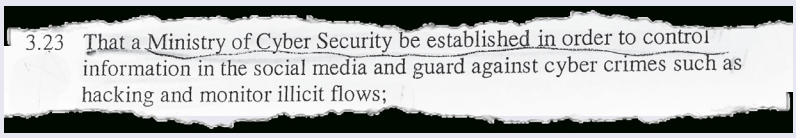

iv) There is a need to urgently implement the requirement for telecommunication service providers to register SIM cards against the name of owners.

v) There is a need to devise mechanism to monitor social media with the aim to detect extremist tendencies and protect the vulnerable sectors of the society from being radicalized.

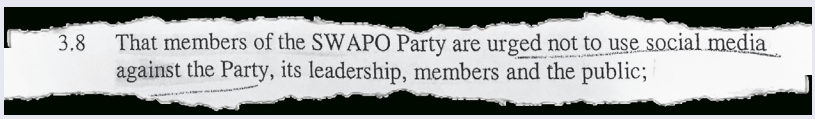
iv) There is a need to urgently implement the requirement for telecommunication service providers to register SIM cards against the name of owners.

v) There is a need to devise mechanism to monitor social media with the aim to detect extremist tendencies and protect the vulnerable sectors of the society from being radicalised.

Similarly, at the end of 2017, at the Swapo Party congress in November that year, amongst the resolutions adopted were the following:


3.23 That a Ministry of Cyber Security be established in order to control information in the social media and guard against cyber crimes such as hacking and monitor illicit flows;

3.23 That a ministry of Cyber Security be established in order to control information in the social media and guard against cyber crimes such as hacking and monitor illicit flows.


3.8 That members of the SWAPO Party are urged not to use social media against the Party, its leadership, members and the public;

3.8 That members of the Swapo Party are urged not to use social media against the party, its leadership, members and the public.

In January 2019, the Minister of Information and Communication Technology (MICT), Stanley Simataa, issued a statement in which he called on Namibians to refrain from insulting the president, ministers and government in general.

"Such derogatory and insulting language directed at the Head of State for that matter is not only contrary to the letter and spirit of the constitution, but also goes against cultural values and norms as human beings and as Africans," Simataa stated.

The minister said that the Namibian government would not be forced into taking drastic steps to curb such behaviour (probably meaning the instruments of state violence), but would use all legal means at its disposal to deal with those who did not comply with the request.

Similar calls and veiled threats by politicians have been made in the past, along with others favouring aggressive regulation of popular social media platforms.

3. QUESTIONING THE STATUS OF 'LAWFUL INTERCEPTION' IN NAMIBIA

When then new Namibian president Hage Geingob announced the appointment of former defence minister Philemon Malima as the new director-general of the Namibia Central Intelligence Service (NCIS) on 30 June 2015, he said: "I will not allow anyone to spy on Namibians, but they (intelligence agency) are just doing their job."[20]

Just over a year earlier, in March 2014, former backbencher of the ruling Swapo Party, Kazenambo Kazenambo, in parliament had accused the NCIS of spying on senior party politicians.

A news report[21] at the time stated: "Kazenambo was persistent with his point that the country was not safe if people were being spied on, adding that there were those who were abusing their powers and spying via phones due to political differences."

He was quoted saying: "We know it's happening. Let's stop it."

Kazenambo was referring to the communications interception and surveillance clauses – in Part 6 – of the Communications Act of 2009[22] allegedly being used to eaves-drop on different factions within the ruling party in the run-up to the November 2014 national and presidential elections. The 2009 Communications Act came into force in 2011 with the creation of the Communications Regulatory Authority of Namibia (CRAN), while regulations for various sections (excluding Part 6) of the law were gazetted over the years since then.

In a subsequent editorial *The Namibian* newspaper stated that then information minister Jöel Kaapanda had "responded in an interview with The Namibian that lawmakers complaining that phones were being tapped should know that they were the ones who passed the Communications Act in 2009".

However, in an interview[23] with another newspaper, the weekly Windhoek Observer, just over three months earlier, in December 2013, Kaapanda had indicated that the interception clauses had not come into force yet as the regulations for Part 6 of the law had not been finalised by then.

20. https://www.namibian.com.na/index.php?page=archive-read&id=138746
21. https://www.namibian.com.na/index.php?id=121406&page=archive-read
22. https://laws.parliament.na/annotated-laws-regulations/law-regulation.php?id=136
23. https://www.observer.com.na/index.php/sports/item/2724-namibia-is-an-open-book

Kaapanda was quoted saying: "You see, one cannot introduce interception without crafting the regulations first, and the crafting of this regulation has taken a bit longer than we anticipated. This is because it involves a number of stakeholders whom we all have to consult regarding the said regulation; the stakeholders are the Internet Service Providers (ISPs). They have to be a part of this process because they are required to comply with the provision that enables us to implement this clause. They would have to look at the equipment within their operations to see whether they meet the requirements of the interception demand. There have been no objections from the stakeholders thus far."

By the time Philemon Malima was appointed as NCIS director-general in mid-June 2015, the regulations for Part 6 of the 2009 Communications Act had still not been finalised.

It appears that mixed signals have consistently been sent about the status of Part 6 of the 2009 Communications Act. These mixed signals were only to become more confusing and telling in another process – Namibia's second periodic review under the International Covenant on Civil and Political Rights (ICCPR) under the auspices of the United Nations Human Rights Committee.

3.1 Spotlight on privacy and communications interception and surveillance during the Universal Periodic Review process

In a process which commenced in 2011, the same year that Namibia's Communications Act of 2009 came into force – with the exception of Part 6 – and ran until mid-2018, Namibia underwent its second periodic review in terms of its general compliance with the International Covenant on Civil and Political Rights (ICCPR).[24]

On 13 October 2014 the Namibian government submitted its initial report to the UN Human Rights Committee (HRC) in Geneva, Switzerland, and on 23 February 2015 the Namibian report was issued publicly by the HRC.

One of the areas of the ICCPR under which Namibia was being reviewed was Article 17 ('The right to respect of privacy, family, home and correspondence, and protection of honour and reputation').

In this regard, the Namibian report [25] stated: "The right to privacy is guaranteed by Article 13 of the Namibian Constitution. The Namibian Constitution provides all citizens with the right to privacy and requires arresting officers to secure a judicial warrant before conducting a search, except in situations of national emergency. The Namibian Parliament passed the Communication Act, Act No.8 of 2009, which provides amongst others for the interception of telecommunications. **However, Part 6 of the Communication Act which provides for the interception of telecommunications is not in operation as yet (own emphasis)**. Part 6 provides for the establishment of interception centers which are necessary for the combating of crime and national security. Interception centres are staffed by such staff members in the Namibia Central Intelligence Service (NCIS) as may be designated by the Director-General with the approval of the Security Commission established by Article 114 (1) of the Namibian Constitution."

Expanding on the explanation, the report stated: "The Communication Act stipulates that before a staff member (NCIS) performs any function in relation to interception or monitoring of telecommunications contemplated in Part 6, he or she must be present before the Judge-President in chambers and make an oath and obtain consent of a judge. The Act makes provision for penalties and offences for contravention of the provisions of the Act."

24. https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx
25. https://tbinternet.ohchr.org/_layouts/treatybodyexternal/Download.aspx?symbolno=CCPR%2fC%2fNAM%2f2&Lang=en

A few months later, in June 2015, international human rights and privacy non-governmental organisation, Privacy International (PI), made a submission[26] to the HRC on these privacy and surveillance issues picked out of Namibia's report to the HRC.
PI stated: "Part 6 of the 2009 Communications Act regulates the 'Interception of Telecommunications'. The 2009 Communications Act directly threatens the respect and protection of privacy rights, as it allows broad powers to the government to monitor telephone calls, e-mail, and internet usage without a warrant. The vague language around references to laws that may require a warrant for any person or institution to intercept or monitor electronic communications or to perform similar activities are baseless, given that even though the law was passed in 2009, **the relevant regulations to implement Part 6 have yet to be adopted (own emphasis)**. In effect this means, that there is no judicial authorisation required to conduct surveillance nor any oversight of any authorisation process."

In effect, what PI pointed out was that there was no way of knowing whether communications monitoring, interception and surveillance was happening or not in Namibia, because there were no mechanisms in place that obligated the reporting on such activities.

Additionally, it stated that: "The obligation the Act places on telecommunications service providers to provide access to their systems and the data of their users without a court order violates the right to privacy. Furthermore, compelling service providers to build into their systems surveillance and monitoring capabilities threatens the integrity, security and privacy of communication systems."

"These provisions provide the framework to allow authorities to conduct mass surveillance of its citizens," stated PI, adding that Part 6 the 2009 Communications Act, if implemented, would undermine the slightly more rigorous judicial oversight authorisation measures in the Namibia Central Intelligence Service (NCIS) Act of 1997.[27]

Two months later, on 21 August 2015, the HRC issued a response [28] to the Namibian report, listing a range of issues with the initial second periodic review report of the country. The HRC, amongst others, questioned the legality of communications monitoring, interception and surveillance.

In this regard the HRC stated: "In relation to paragraph 185 (quoted earlier from the Namibian report) of the State party's report, please provide updated information on the establishment of interception centres provided for in Part 6 of the Communications Act, 2009 (Act No 8 of 2009), and provide detailed information on the gathering and holding of private information under the Act or under any other laws. Please also indicate whether and following what procedure individuals have the right to ascertain what personal data concerning them is stored and for what purpose, and to request rectification or elimination of such data. Please indicate the remedies available to complainants of a violation under article 17 in such contexts."

On 30 November 2015, Namibia sent a reply[29] to the HRC. Notably, the Namibian government's response refers to "unlawful interception" and "lawful interception" and once again states that the relevant section of the law which deals with interception had not been implemented yet.

The response stated: "Section 70 of the Communications Act, (Act 8 of 2009) provides for establishment of interception centers. **Part 6 of the Act has not yet entered into force (own emphasis)**. However, the interception addressed in the Communications Act has nothing sinister about it, safe for securing the peace, order, stability and safety of the Namibian nation."

26. https://privacyinternational.org/sites/default/files/2017-12/Namibia%20UPR_PI_submission_FINAL.pdf
27. https://laws.parliament.na/cms_documents/namibia-central-intelligence-service-372a55b6b9.pdf
28. https://tbinternet.ohchr.org/_layouts/treatybodyexternal/Download.aspx?symbolno=CCPR%2fC%2fNAM%2fQ%2f2&Lang=en
29. https://tbinternet.ohchr.org/_layouts/treatybodyexternal/Download.aspx?symbolno=CCPR%2fC%2fNAM%2fQ%2f2%2fAdd.1&Lang=en

The Namibian response stated that section 70 of the law provided for the president to establish interception centres to combat crime and for 'national security'. "In attempting to ensure that interception centres are not abused, the legislator [probably supposed to be legislation] in Section 70 (3) provides that any staff member, before performing any function relating to interceptions must take an oath before the Judge-president in chambers," it was reiterated, and pointed out that the oath was to "ensure that no one carries out an unlawful interception".

The response also dealt with the treatment of confidential information, but did not address most of the substantive concerns raised by the HRC – such as answering whether interception centres existed, and about the retention, storage and management of intercepted data and measures to ensure how it could be determined whether an intercept was lawful or not.

Three months later, in February 2016, a group of Namibian civil society organisations, led by the Namibian Non-Governmental Organisations Forum (NANGOF) Trust and the Legal Assistance Centre (LAC), submitted a CSO report[30] in response to the government's report of a year earlier.

On the issue of communications monitoring, interception and surveillance, the report stated: "There have been anecdotal reports of active interception of telecommunications. These include the tapping of telephones and "bugging" of offices. It is not possible to scientifically verify such reports. The State party under paragraph 185 of its State Report states that interception centres are staffed by the Namibia Central Intelligence Service (NCIS) as designated by the Director-General. The use of the word "are" and not "will be" can cause the inference to be drawn that **the interception centres are currently operational despite the enabling part of the legislation not yet having come into force (own emphasis).** It is noted that the Committee's further questions pertaining to the type of information obtained, the individual's right to access such personal information and possible remedies available, were not addressed by the State party under reply."

The following month, on 8 and 9 March 2016, a Namibian delegation, led by then-justice minister Albert Kawana[31] , attended the 116th session of the HRC, at Geneva, Switzerland, to give feedback about various aspects of the Namibian report as questioned by the HRC and the issues raised by other parties. On 9 March the Namibian delegation was questioned[32] about the concerns around communications monitoring, interception and surveillance, specifically "whether the interception centres referred to in paragraph 185 of the report (CCPR/C/NAM/2) were now operational".

Furthermore, the HRC once again wanted to know about what privacy protections and oversight measures were in place to prevent surveillance abuse.

In response, justice minister Kawana merely stated: "Under the Communications Act, information could not be intercepted without judicial authorisation. In accordance with article 18 of the Constitution, any individual who was aggrieved by the act of a public official had the right to seek redress."

What Kawana once again did not address was whether Part 6 was being used for surveillance purposes, how an individual would even know that there had been a breach of their privacy for such purposes, as well as the concerns around data retention and storage.

30. https://tbinternet.ohchr.org/_layouts/treatybodyexternal/Download.aspx?symbolno=INT%2fCCPR%2fCSS%2fNAM%2f23130&Lang=en
31. Since February 2018 Kawana has been Attorney-General following a Cabinet reshuffle.
32. https://documents-dds-ny.un.org/doc/UNDOC/GEN/G16/047/98/PDF/G1604798.pdf?OpenElement

At the end of the HRC proceedings, the chairperson [a Mr. Salvioli] expressed some dissatisfaction with the nature of the responses from the Namibian delegation, with the record of proceedings stating: "Unfortunately, the [Namibian] delegation's rather general replies to those questions would be of limited use to the Committee in the formulation of its concluding observations. Consequently, he [Salvioli] hoped that the delegation would be able to provide more detailed responses in writing within 48 hours of the closure of proceedings."

The next day, on 10 March 2016, the Namibian government responded[33] with a brief statement on some of the issues raised during the two days of the HRC session, but notably nothing further was said about interception centres or the provisions of the Communications Act.

More than a month later, on 22 April 2016, the HRC publicly issued its concluding observations[34] about Namibia's second periodic review report.

On the issue of "Monitoring, surveillance and interception of private communication" the HRC concluded: **"The Committee notes with concern that interception centres seem operational despite the fact that their legal basis, part 6 of the Communications Act (Act No. 8 of 2009), is not yet in force (own emphasis).** While noting the indication by the delegation that all interceptions must be authorised by a magistrate, and that no private information is kept, the Committee is concerned about the lack of clarity regarding the reach of legal interception possibilities, as well as about the safeguards to ensure respect of the right to privacy in line with the Covenant (arts.17 and 21)." It further recommended that: "The State party should ensure that the interception of telecommunications may only be justified under limited circumstances authorised by law with the necessary procedural and judicial safeguards against abuse, and supervised by the courts when in full conformity with the Covenant."

On 8 August 2017, more than a year after the 'concluding observations' were made, the HRC wrote[35] to the Namibian government to request a response to its final remarks. The correspondence stated that "The Committee would appreciate receiving the above-mentioned information by 8 November 2017.

"The State party is kindly requested, when submitting its reply to the Committee, not to reiterate information that has already been provided to the Committee, but rather to focus on the measures taken to implement the recommendations selected for the follow-up procedure since the adoption of the concluding observations."

On 10 July 2018, almost a year after the HRC's request for a response and nine months over the 8 November 2017 deadline, the last follow-up correspondence[36] was received from Namibia, and once again nothing further was said about interception centres or the provisions of the Communications Act.

Based on this, and especially judging by the Namibian government's refusal to comment further on whether communications monitoring, interception and surveillance were happening and on the status of interception centres, it can be reasonably concluded that there is some credibility to claims that communications monitoring, interception and surveillance are happening and that such centres exist and are operational. These claims gain traction especially when considered against the communications interception and surveillance technology procurement activities of the Namibia government over the last decade.

33. https://tbinternet.ohchr.org/_layouts/treatybodyexternal/Download.aspx?symbolno=INT%2fCCPR%2fAIS%2fNAM%2f23256&Lang=en
34. https://tbinternet.ohchr.org/_layouts/treatybodyexternal/Download.aspx?symbolno=CCPR%2fC%2fNAM%2fCO%2f2&Lang=en
35. https://tbinternet.ohchr.org/_layouts/treatybodyexternal/Download.aspx?symbolno=INT%2fCCPR%2fFUL%2fNAM%2f28392&Lang=en
36. https://tbinternet.ohchr.org/_layouts/treatybodyexternal/Download.aspx?symbolno=CCPR%2fC%2fNAM%2fCO%2f2%2fAdd.1&Lang=en

However , before going any further, the status of Part 6 of the Communications Act of 2009 needs to be clarified. At a stakeholder briefing meeting, titled 'Industry Roundtable Discussion on Combating Online Child Sexual Abuse in Namibia', on 13 February 2019 at Windhoek's Thüringerhof Hotel, the Director of ICT Development in the Ministry of Information and Communication Technology, Linda Aipinge, when questioned about the status of Part 6 of the Communications Act, stated that Part 6 has still not been implemented as the regulations for it had not been finalised yet. However, she did indicate that the finalisation of the regulations for Part 6 had become urgent and it was conceivable that they would still be gazetted during 2019.[37]

3.2 Key observations

- The Namibian government has emitted mixed signals about the implementation status of Part 6 (Interception of Telecommunications) of the Communications Act of 2009 for most of the last decade;
- However, the government has publicly maintained that Part 6 had not come into force and by February 2019 that appeared to still be the case, as regulations concerning Part 6 had still not been finalised;
- The Namibian government's refusal to respond substantively to concerns about communications monitoring, interception and surveillance by the UN Human Rights Committee, could reasonably be interpreted to mean that interception centres exist and are operational, as has been alleged by others;
- Thus, the legality of state communications monitoring, interception and surveillance activities remains highly questionable, a decade after the Communications Act was enacted.

Namibian laws enabling communications interception and surveillance

There are a number of laws on the Namibian statute books that enable or have a significant bearing on communications monitoring, interception and surveillance in some form or other, whether as part of evidence gathering in criminal matters or telecommunications interception for anti-terrorism purposes.

These laws are:

- Criminal Procedure Act of 1977[38]
- Protection of Information Act of 1982
- Police Act of 1990
- Namibia Central Intelligence Service Act of 1997
- Communications Act of 2009
- Financial Intelligence Act of 2012
- Prevention and Combating of Terrorist and Proliferation Activities Act of 2014

37. The author was at this meeting and witness to this discussion.
38. In early February 2019, the Speaker of the National Assembly, Peter Katjavivi, announced that the Criminal Procedure Repeal Act of 2018 had been passed in 2018 to do away with the old law from 1977.

4. ARE NAMIBIANS BEING SPIED ON 'UNLAWFULLY'?

With there being credible indications, as discussed in the previous section, that communications monitoring, interception and surveillance are happening under the auspices of the Namibia Central Intelligence Service (NCIS), while Part 6 of the 2009 Communications Act has not entered into force yet, it can be reasonably concluded that the legality of such activities is highly suspect and a clear violation of the right to privacy as constitutionally enshrined. That is to say, surveillance overreach and abuse appear to be realities in Namibia.

This is because for most of the last decade, from 2009 to the beginning of 2019, the Namibian government, or state security and intelligence operatives, has been very active in the surveillance technology market as a buyer or potential buyer of all sorts of surveillance tech. The question that comes to mind is: With Part 6 of the Communications Act not in force yet, why have certain Namibian government agencies and actors been shopping around internationally for communications monitoring, interception and surveillance technologies for more than a decade? It seems unlikely that these technologies are being stockpiled for the eventual implementation of Part 6, if ever, as communications technologies generally become obsolete very quickly. It can surely only be that such technologies procured since 2009, and even earlier, have been purchased and used, as has been alleged.

Much of the information around Namibian state security's activities in the surveillance tech marketplace is obtained from sources that have mined military equipment and technology export licence data of the European Union, the United Kingdom and the United States, as well as other Western nations, which are relatively transparent about such exports. Some of the information was also obtained by these sources through freedom of information requests to relevant authorities in their countries. What follows mostly relies on the database of the UK-based Campaign Against Arms Trade (CAAT) and primarily looks at Namibian government surveillance tech exports from the UK and the UK-based subsidiaries of companies from other European or Western countries.

Communications interception versus surveillance [39]

Interception: Interception of communications takes two forms: the collection and monitoring of communications data (e.g. records of who contacted whom, when, from where and for how long); and, the acquisition (including listening, viewing and diversion) of the content of the communications themselves, to a person other than the sender or recipient or intended recipient of that communication.

Surveillance: This encompasses a broad range of activity involving (electronic) communications networks. It includes not only the actual reading of private communications by another human being, but also the full range of monitoring, interception, collection, analysis, use, preservation and retention of, interference with, or access to information that includes, reflects, or arises from a person's communications in the past, present, or future.

Source: The Surveillance State: Communications surveillance and privacy in South Africa, Right2Know, March 2016.

39. https://www.mediaanddemocracy.com/uploads/1/6/5/7/16577624/sa_surveillancestate-web.pdf

4.1 Following the trails of Namibia's spy tech procurement forays

The UK-based Campaign Against Arms Trade (CAAT),[40] which has been monitoring mostly UK arms exports since the early 1970s, estimates that from January 2008 to September 2018, British firms or firms based in Britain applied for 59 export licences to Namibia for military and dual-use [41] goods (gear, equipment, ammunition, technology) valued at over 86 million[42] British pounds (which, considering the exchange rate fluctuations would be worth somewhere between N$1.2 billion – N$1.5 billion over the same time period).

However, most of this value, about 72.5 million[43] British pounds (±N$1.2 billion), represents "information security equipment" and "software for information security equipment" for which a standard individual export licence (SIEL), with a "telecommunications and information security" rating, to Namibia was approved in June 2016, according to the CAAT database.

Notably, during the period that Namibia's second periodic report was undergoing evaluation and discussion within UN Human Rights Committee (HRC) processes, from about February 2015 to July 2016, four SIELs (see Image 4) were approved for telecommunications interception equipment to Namibia. It was during this period that the Namibian government twice indicated – with the public release of the country's periodic report on 23 February 2015 and in November 2015 – that **"Part 6 of the Communication Act which provides for the interception of telecommunications is not in operation as yet (own emphasis)".** [44]

Image 4: Campaign Against Arms Trade

Licences

4 results

Date ▲▼	Type	Country ▲▼	Item	Revoked	Rating	Value ▲▼
2016-07-15	SIEL	Namibia	telecommunications interception equipment (notes)		5A001	£35,000
2016-01-25	SIEL	Namibia	telecommunications interception equipment T		5A001	£10,000
2015-11-11	SIEL	Namibia	telecommunications interception equipment		5A001	£55,142
2015-03-09	SIEL	Namibia	components for telecommunications interception equipment T software for telecommunications interception equipment T telecommunications interception equipment T		5A001 5D001	£32,453 £2,811

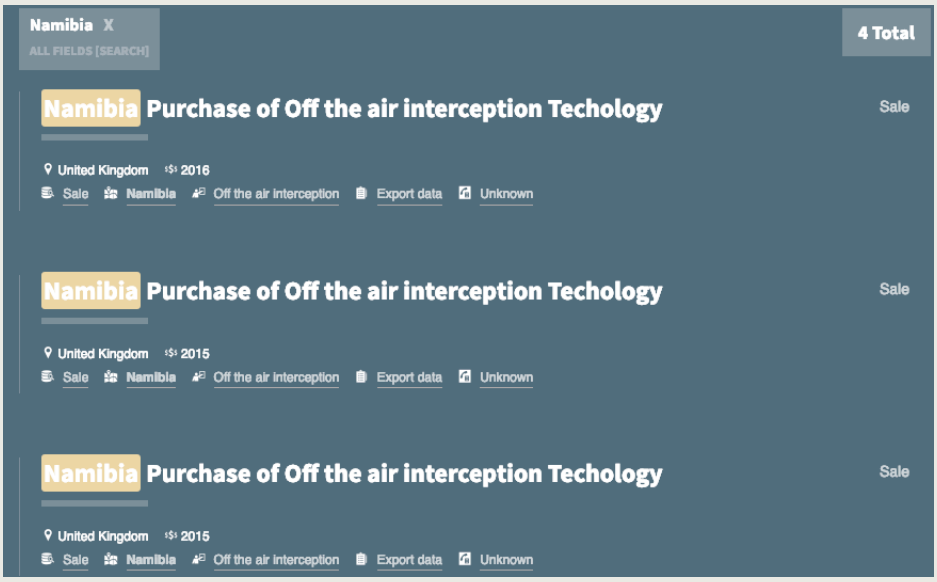
4 results

Even more striking, as Image 4 indicates, in November 2015 an export licence was approved for the export of telecommunications interception equipment to Namibia, while that same month the Namibian government responded to HRC concerns about interception centres being active by stating: "Section 70 of the Communications Act, (Act 8 of 2009) provides for establishment of interception centers. **Part 6 of the Act has not yet entered into force (own emphasis).** However, the interception addressed in the Communications Act has nothing sinister about it, safe for securing the peace, order, stability and safety of the Namibian nation."

This information is backed up by information available on the Surveillance Industry Index website[45] which also shows (see *Image 5* below) the purchase of "off the air interception technology" by Namibia during that same 2015-2016 period.

40. https://www.caat.org.uk/
41. Dual-use goods are goods which can be used for both military and civilian purposes. Surveillance equipment and technologies are mostly in the dual-use category.
42. https://www.caat.org.uk/resources/export-licences/licence?use=all&region=Namibia
43. https://www.caat.org.uk/resources/export-licences/licence?use=all&region=Namibia&date_from=2016-06&date_to=2016-06
44. See 3.1 in the previous section.
45. https://sii.transparencytoolkit.org/search?utf8=%E2%9C%93&q=Namibia

Image 5: Surveillance Industry Index



"Off the air interception technology" refers to what are colloquially called 'grabbers', but which are more commonly known in the surveillance industry as IMSI-catchers. According to a Motherboard article from August 2016, "IMSI-catchers typically extract the phone SIM card's unique identifying number, or IMSI, but many models are capable of more powerful surveillance techniques as well" and "can be used to intercept SMS messages and voice calls from mobile phones".

The same article quotes Claudio Guarnieri, a technologist at international human rights organisation Amnesty International, as saying: "IMSI catchers are probably one of the most controversial and yet more demanded pieces of surveillance technology marketed today. They are of dubious legality and their use raises serious ethical and privacy concerns due to their invasiveness and wide reach."[46]

However, it's not only in the UK that Namibia has been looking to buy or has bought communications surveillance technologies, for it seems efforts have been made to procure such technologies or services in other European Union (EU) states as well.

According to a June 2015 report[47] by the Coalition Against Unlawful Surveillance Exports (CAUSE), the Namibian government attempted to buy internet surveillance technologies in Switzerland in 2013, but by then the Swiss government had become concerned about such technologies being used for repressive purposes by some states and clamped down on the export of such technologies by Swiss-based companies. Consequently, "in early 2014 several companies withdrew their applications for licences to export internet monitoring technology from Switzerland. As a result, exports to Ethiopia, Indonesia, Yemen, Qatar, Malaysia, **Namibia**, two licences for Oman, Russia, Chad, Taiwan, Turkmenistan, UAE, and China did not go ahead".

Similarly, the Namibian government attempted to procure internet monitoring technology or hacking services from an Italian firm from October 2014 – incidentally, the same month that Namibia submitted its second periodic review report to the HRC – to mid-2015 (see HackingTeam under 4.2). This was in the period that Namibia's periodic review report was before the HRC and during which the Namibian government continually denied that interception centres were in existence and operational. This attempt seems to have stalled following a data breach and a Wikileaks expose that eventually led to the Italian government revoking the Italian firm's ability to export its intrusion malware.

46. https://motherboard.vice.com/en_us/article/4xaq4m/the-uk-companies-exporting-interception-tech-around-the-world
47 https://www.fidh.org/IMG/pdf/cause_report_final.pdf

According to CAAT, in 2011 and between 2015 and 2017, the Namibian government also seems to have done business with the UK-based subsidiary of a Danish firm, Systematic, which through its "business unit for Intelligence & National Security delivers solutions, services and know-how for surveillance, prevention, analysis, threat assessment and crisis handling".

Aside from European firms, in 2015, communications interception and surveillance technology was also sourced from a Canadian firm, Octasic, also through its UK-based arm, for a mobile device interception and monitoring system referred to as 'Mongoose' (see Image 6 below).

Image 6: Octasic communications interception and surveillance technology

However, as earlier stated, while EU nations are somewhat transparent about weapons and surveillance technology exports, other countries in other parts of the world are not. Chinese technology giants Huawei and ZTE have been major operators in the Namibian telecommunications space for over a decade, and in fact, in 2018 Huawei and Namibia's largest mobile telephony and internet service provider Mobile Telecommunications Company (MTC), marked 10 years of technology partnership, with Huawei equipment forming the backbone of Namibia' mobile networks.

Huawei is not only the world's largest maker and distributor of telecommunications equipment, but also the world's largest maker and distributor of surveillance technologies and equipment. It should be noted that, in a continental scandal from late 2017 to early 2018, Huawei was implicated in enabling alleged Chinese government spying on the African Union headquarters in Addis Ababa, Ethiopia.

Over the last decade, both Huawei and ZTE have been accused on numerous occasions by Western governments and intelligence agencies of cooperating with Chinese state security, but evidence of 'backdoors' for Chinese surveillance have never been made public and the companies have denied any claims of enabling spying by the surveillance-obsessed Chinese state.

Against this backdrop, the extent to which Huawei and ZTE are involved with or enabling Namibian state surveillance practices and activities is a point of concern.

Image 7: Some of the licences granted by the British government for surveillance equipment exports to Namibia.

SIEL (Temporary)	ISSUE, NLR	Namibia	components for telecommunications interception equipment, software for telecommunications interception equipment, telecommunications interception equipment	5A001f1, 5D001a, NLR	1: Evolve4-Nimbus system with 4 x EURO band TRXs, 2: Evolve4-Nimbus Support for UMTS protocol, 3: Evolve4-Nimbus Option - Channel Activation, 4: Evolve4-Nimbus - 900MHz Band Support, 5: Evolve4-Nimbus - 1800MHz Band Support, 6: Evolve4-Nimbus - 2100MHz Band Support, 7: UMTS Option - 3G Blind Call, 8: UK Cloverleaf Power Cable - fitted with 5Amp Fuse, 9: Euro Cloverleaf Power Cable, 10: US CloverLeaf Power Cable, 11: Evolve4 Nimbus Desktop PSU, 12: 8GB transcend Jet Flash 300 USB 2.0 Flash Drive, 13: GPS Splitter ZAPD-2DC-S+, 14: UK Plug to IEC C19 Socket - 13A Fuse - 2.5m, 15: Euro Plug to IEC C19 Socket - 2.5m, 16: US Plug to IEC C19 Socket - 2m, 17: 0.8GHz - 2.2GHz Omni Antenna, 18: Getac Laptop, 19: Lind DC Power Adapter for Getec Laptop, 20: Antenna, 2.4GHz, Whip, Reverse SMA with 90deg Joint, 21: GPS Antenna Dual Saw HR Filter with SMA Connector, 22: XPZ 6M LMR 195 N-N Cable, 23: XPZ 2M LMR195-UF SMA-Type to SMA, 24: 3GNE Battery Power Cable, 25: 3GNE Desktop PSU Power Cable, 26: Nimbus Unit - GPS Splitter Cable, 27: NST Unit - GPS Splitter Cable, 28: Nimbus Ethernet Cable, 29: Nimbus Battery Link Cable, 30: Evolve4-Nimbus Support for LTE protocol, 31: UMTS Option - Push to 3G	COMPLETED
SIEL (Permanent)	ISSUE	Namibia	telecommunications interception equipment	5A001f2	1: Searchlight UMTS/GSM Detection and Location system	COMPLETED
SIEL (Temporary)	ISSUE	Namibia	telecommunications interception equipment	5A001f2	1: Modified OCTBTS 8000 Portable Base Station System known as "Mongoose"	COMPLETED
SIEL (Temporary)	ISSUE, NLR	Nigeria	components for telecommunications interception equipment, software for telecommunications interception equipment, telecommunications interception equipment	5A001f1, 5D001a, NLR	1: Evolve4-Nimbus System - 4 Channel EU-LTE1, 2: Evolve4-Nimbus Channel Activation, 3: Evolve4-Nimbus Mapplication Software Option, 4: Evolve4-Nimbus - Support for GSM Protocol, 5: Evolve4-Nimbus - Support for UMTS Protocol, 6: Evolve4-Nimbus - LTE Profile Activation, 7: Evolve4-Nimbus 800MHz Band Support, 8: Evolve4-Nimbus 900MHz Band Support, 9: Evolve4-Nimbus 1800MHz Band Support, 10: Evolve4-Nimbus 2100MHz Band Support, 11: Evolve4-Nimbus Software Option - Service Denial, 12: Evolve4-Nimbus - Push to UMTS/GSM Software Option, 13: UMTS Option - Push to 2G Software Option, 14: 3G Blind Call Software Option, 15: 2G Blind Call Software Option, 16: SMS Interception Software Option, 17: Nimbus Unit - GPS Cable, 18: 3GNE Battery Power Cable, 19: Nimbus Ethernet Cable	COMPLETED

Mass versus targeted communications surveillance[48]

Mass surveillance: This is the subjection of a population or significant component of a group to indiscriminate monitoring. Any system that generates and collects data without attempting to limit the dataset to well-defined targeted individuals is a form of mass surveillance and it increasingly involves the generation, collection, and processing of information about large numbers of people.

Targeted surveillance: This is surveillance directed at particular individuals. Targeting methods include the interception of communications and the use of communications data.

Source: The Surveillance State: Communications surveillance and privacy in South Africa, Right2Know, March 2016.

4.2 'Enemies of the Internet' and Namibia

In March 2013, international journalism watchdog Reporters Without Borders in a special report[49] for the first time labelled five companies – Gamma Group, Trovicor, HackingTeam, Amesys and Blue Coat – as 'Corporate Enemies of the Internet' and "digital era mercenaries", "because they sell products that are used by authoritarian governments to commit violations of human rights and freedom of information". Indications are that the Namibian state has had dealings with at least two – Gamma Group and HackingTeam – of the 'Corporate Enemies of the Internet' in recent times.

48. https://www.mediaanddemocracy.com/uploads/1/6/5/7/16577624/sa_surveillancestate-web.pdf
49. surveillance.rsf.org/en

Gamma Group

Image 8: Gamma Group

According to the company's website: "Gamma Group is an international manufacturer of surveillance & monitoring systems with technical and sales offices in Europe, Asia, the Middle East and Africa. We provide advanced technical surveillance, monitoring solutions and advanced government training as well as international consultancy to National and State Intelligence Departments and Law Enforcement Agencies."

Gamma Group[50], an Anglo-German company, is the maker of the notorious FinFisher spyware, which since 2012[51] has been identified as being actively used by various repressive regimes around the world to spy on journalists, dissidents and democracy activists, as well as citizens in general. In 2014 Gamma Group was hacked and its FinFisher suite was exposed through Wikileaks.[52]

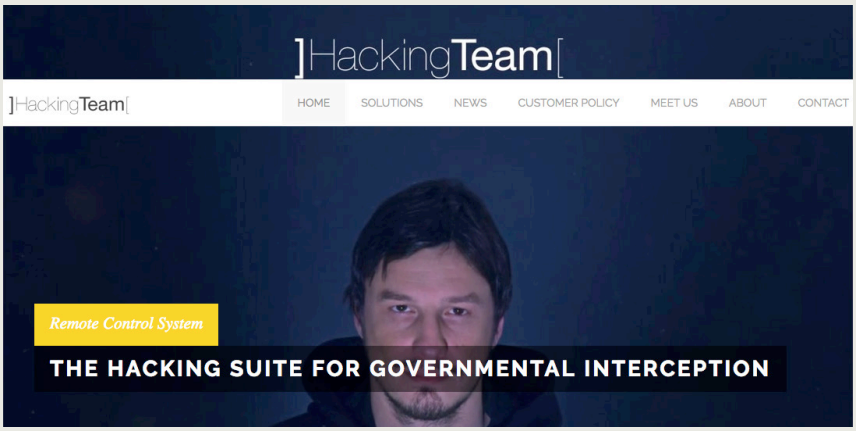
According to the Campaign Against Arms Trade (CAAT), Gamma Group first applied for a military export license to Namibia in 2010, but indications are that it has applied for such licenses over the intervening years as well, as CAAT indicates that it also applied for a license between 2015 and 2017.

The Coalition Against Unlawful Surveillance Exports (CAUSE) stated in a 2015 report: "As detailed in a Gamma International brochure describing their suite of systems, FinFly LAN and FinFly ISP are able to infect files that are downloaded by the target, infect the target by sending fake software updates for popular software or infect the target by injecting the Payload into visited websites. The result of such a download is that the computer or mobile phone device is infected, allowing full access to information held on it. It is for instance possible to access emails, social media messaging and Skype calls. It also enables the entity doing the targeting to remotely operate microphones and webcams or cameras on computers and mobile phones."

50. https://rsf.org/en/news/special-report-internet-surveillance-focusing-5-governments-and-5-companies-enemies-internet
51. https://citizenlab.org/2012/07/from-bahrain-with-love-finfishers-spy-kit-exposed/
52. https://wikileaks.org/spyfiles4/customers.html

HackingTeam

Image 9: HackingTeam



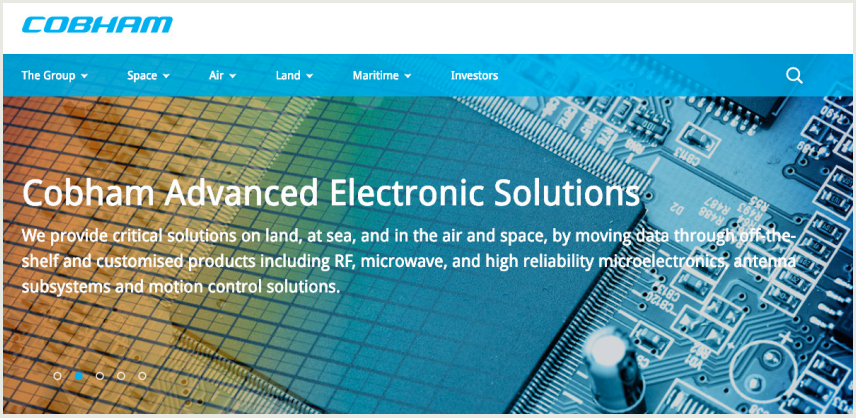
Until late 2015, HackingTeam was an Italian-based "purveyor of offensive intrusion and surveillance capabilities to governments, law enforcement agencies and corporations"[53] – basically malware for state security and intelligence agencies to break into and monitor individuals' private communications devices and systems.

Like Gamma Group, HackingTeam also suffered a damaging hack and a data leak through Wikileaks, in mid-2015. It was through this leak that its dealings with various state security and intelligence agencies, including Namibia's,[54] across the world was exposed.

The Coalition Against Unlawful Surveillance Exports (CAUSE) stated in 2015 about HackingTeam's Remote Control System (RCS) malware: "Once a computer is infected with malware, it is possible for the individual who sent the malware to read all email correspondence, search through documents saved on the computer, and monitor web surfing, including communications via social media. Operators can literally see ideas being formed as they are typed; they have access to family photos, personal correspondence and other sensitive personal information. At this stage, changing passwords or using encryption has no effect on the interception. Some forms of malicious software even allow for the possibility to remotely switch on the microphone and camera of the device (computer / smartphone) so conversations in the vicinity of the computer can be listened to".

Cobham

Image 10: Cobham



53. https://www.revolvy.com/page/Hacking-Team
54. To read about Namibia's dealings with HackingTeam go to: https://www.namibian.com.na/175475/archive-read/The-rise-of-the-Namibian-surveillance-state

Another company that deserves mention and scrutiny is British IMSI-catcher manufacturer, Cobham, which according to Wikileaks was also a "distribution partner", through its German arm, Cobham Surveillance GmbH, for Gamma Group's FinFisher spyware suite.

The Surveillance Industry Index lists[55] Cobham, which is 49th amongst the 50 largest military and defence contractors in the world, as making "Monitoring Centre, Phone Monitoring, Audio Surveillance, Video Surveillance, Location Monitoring, Equipment, Monitoring Centres, and Technical Surveillance technology".

In 2015, Cobham or a distributor of Cobham equipment applied for an export licence to Namibia for its Evolve-4 Nimbus IMSI-catcher (Image 10) and according to an online report,[56] "the UK government granted exports related to the Cobham device to Algeria, Brazil, Colombia, Macedonia, **Namibia**, Oman, Paraguay, Qatar, Singapore, Turkmenistan, and the United Arab Emirates. Some of these, like the licence to Macedonia, were for temporary exports, meaning the export was likely for a demonstration to a customer or a trade show. Other licences were for permanent export".

Image 11: Cobham's Evolve-4 Nimbus IMSI-catcher

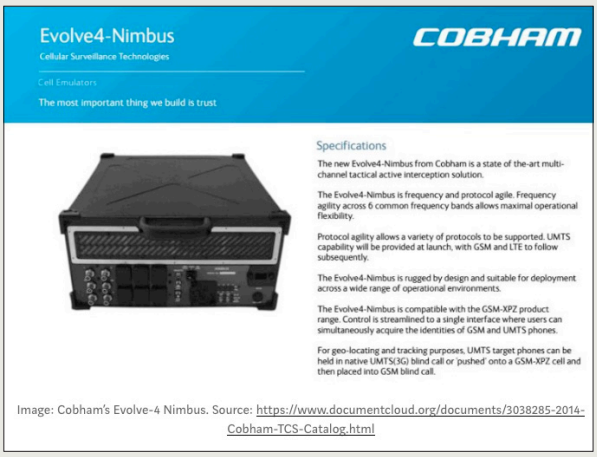


Image: Cobham's Evolve-4 Nimbus. Source: https://www.documentcloud.org/documents/3038285-2014-Cobham-TCS-Catalog.html

The article also states that: "The licence for temporary export to Turkmenistan also mentions another Cobham IMSI-catcher mentioned in the Cobham brochure: the GSM-XPZ PV. The Nimbus licenscs for Algeria, **Namibia**, and Qatar also include a reference to "XPZ."

Image 12: Cobham's GSM-XPZ PV IMSI-catcher

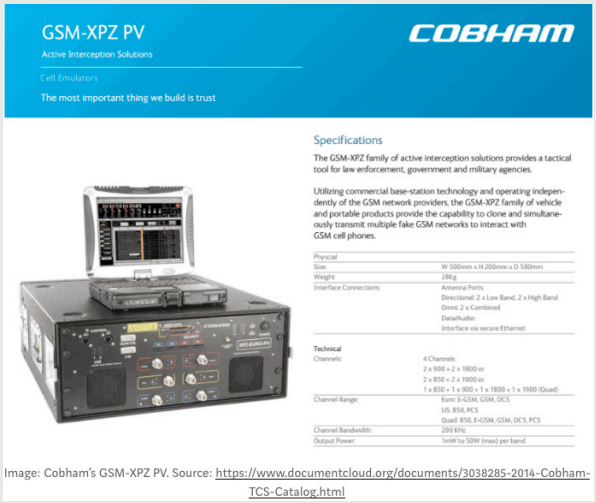


Image: Cobham's GSM-XPZ PV. Source: https://www.documentcloud.org/documents/3038285-2014-Cobham-TCS-Catalog.html

55. https://sii.transparencytoolkit.org/search?utf8=%E2%9C%93&utf8=%E2%9C%93&q=Cobham
56. https://spytechexports.com/plotting-the-spread-of-uk-made-imsi-catchers-963d6979d5cf

The article continues that "the GSM-XPZ PV, according to the brochure, is capable of phone call and SMS interception. The listing also includes Mapplication, Cobham's analysis software for data collected by these sorts of devices".

According to the Campaign Against Arms Trade (CAAT), Cobham also applied for a military export licence to Namibia in 2011.

It is not known if these exports went ahead. The concern here is that if these technologies have been delivered to Namibia, then the country's state security and intelligence apparatus has access to powerful communications interception and surveillance technologies. The question remains: Are such technologies being utilised while the primary legal framework, Part 6 of the 2009 Communications Act, has not been brought into force yet?

And based on all the circumstantial evidence presented here, the answer would seem to lean worryingly to the affirmative.

4.3 Key observations:

- Security and intelligence elements within the Namibian government have been acquiring or looking to acquire communications monitoring, interception and surveillance technologies and equipment since before 2009;
- Much of the information concerns Namibian efforts to procure communications interception and surveillance technologies and equipment from firms based in the European Union (EU) and the UK;
- There is very little information available about Namibia's engagements and dealings with Chinese vendors of communications interception and surveillance technologies and equipment;
- The question is whether sophisticated communications interception and surveillance capabilities are being deployed despite Part 6 of the 2009 Communications Act not yet being implemented?

TABLE 1: Campaign Against Arms Trade (CAAT) records[57] of UK government approved export licences to Namibia for communications surveillance and intelligence gathering related technologies.

DATE	LICENCE	COUNTRY	ITEM	VALUE
2018-05-11	SIEL	Namibia	information security equipment	£33,000
2018-05-11	SIEL	Namibia	information security equipment	£33,000
2018-03-28	SIEL	Namibia	information security equipment	£33,000
2017-08-18	SIEL	Namibia	information security equipment	£33,000
2016-07-15	SIEL	Namibia	telecommunications interception equipment	£35,000
2016-06-06	SIEL	Namibia	information security equipment software for information security equipment	£70,488,726 £2,069,497
2016-02-29	OIEL	Namibia	information security equipment information security software software for information security equipment software for information security software technology for information security equipment technology for information security software technology for software for information security equipment technology for software for information security software	Unlimited
2016-01-25	SIEL	Namibia	telecommunications interception equipment T	£10,000
2015-11-11	SIEL	Namibia	telecommunications interception equipment	£55,142
2015-04-29	OIEL	Namibia	components for information security equipment information security equipment information security software software for information security equipment technology for information security equipment technology for information security software	Unlimited
2015-03-09	SIEL	Namibia	components for telecommunications interception equipment T software for telecommunications interception equipment T telecommunications interception equipment T	£32,453 £2,811

57. https://www.caat.org.uk/resources/export-licences/licence?use=dual&region=Namibia&n=0

DATE	LICENCE	COUNTRY	ITEM	VALUE
2014-08-18	SIEL	Namibia	equipment employing cryptography	£1,006
2014-07-15	SIEL	Namibia	equipment employing cryptography	£961
2014-07-10	SIEL	Namibia	equipment employing cryptography	£3,010
2014-05-27	SIEL	Namibia	equipment employing cryptography	£4,871
2014-03-10	SIEL	Namibia	equipment employing cryptography	£13,084
2013-10-16	SIEL	Namibia	equipment employing cryptography	£19,306
2013-07-18	SIEL	Namibia	equipment employing cryptography	£1,000
2013-06-03	SIEL	Namibia	equipment employing cryptography	£9,676
2013-05-28	SIEL	Namibia	equipment employing cryptography	£9,676
2013-04-25	SIEL	Namibia	cryptographic software equipment employing cryptography	£1,650 £403
2013-03-20	SIEL	Namibia	equipment employing cryptography	£18,108
2011-04-08	SIEL	Namibia	radio jamming equipment software for the use of radio jamming equipment	£236,463 £1,500
2010-10-13	SIEL	Namibia	radio jamming equipment T	£15,000
2009-08-11	OIEL	Namibia	cryptographic software equipment employing cryptography software for the use of equipment employing cryptography technology for the use of equip-ment employing cryptography	Unlimited
2008-07-28	OIEL	Namibia	components for equipment employing cryptography cryptographic software equipment employing cryptography software for the use of equipment em-ploying cryptography technology for the use of cryptograph-ic software technology for the use of equipment employing cryptography	Unlimited

SIEL = Standard Individual Export Licence; OIEL = Open Individual Export Licence
All these exports are classified as 'Dual-use: telecommunications and information security'

5. EXPOSING STATE SURVEILLANCE ABUSE - WHY IT MATTERS

The issue of surveillance, by both states and private actors, has been a subject of growing scholarship and international human rights discourse over the last two decades, especially as the internet and mobile phones have become near ubiquitous across large parts of the world.

As communications technologies have spread, and the ease of surveillance has increased equally exponentially, surveillance scholars have come to settle on some certainties in the 'age of surveillance', specifically that a) surveillance abuse, by both state and private actors, is a commonplace occurrence; and b) that basic human rights are being undermined and violated by widespread surveillance all the time.

In a 2016 report[58] South Africa's Right2Know campaign summed up the situation, after the exposure of large-scale state surveillance abuse in that country, as follows: "Surveillance can have a hugely chilling effect on political activism, protest, debate, investigative journalism and the practice of human rights law and thus the overall character of critical democratic engagement, dissent and the ability of weaker groups to question and challenge those with/in power."

And in his seminal paper,[59] *The Dangers of Surveillance*, from 2013, American privacy expert Neil M. Richards, stated: "Shadowy regimes of surveillance corrode the constitutional commitment to intellectual freedom that lies at the heart of most theories of political freedom in a democracy. Secret programs of wide-ranging intellectual surveillance that are devoid of public process and that cannot be justified in court are inconsistent with this commitment and illegitimate in a free society."

Two years earlier and almost a decade ago now, the situation had already become so disturbing that in 2011, UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue, issued a report[60] stating: "The Special Rapporteur is deeply concerned by actions taken by States against individuals communicating via the Internet, frequently justified broadly as being necessary to protect national security or to combat terrorism. While such ends can be legitimate under international human rights law, surveillance often takes place for political, rather than security reasons in an arbitrary and covert manner. For example, States have used popular social networking sites, such as Facebook, to identify and to track the activities of human rights defenders and opposition members, and in some cases have collected usernames and passwords to access private communications of Facebook users."

La Rue also pointed to states attempting various means to undermine device and software security, including by limiting the use of encryption measures and technologies, in order to enable arbitrary and mass surveillance. La Rue's report to the UN Human Rights Committee (HRC) came nearly two years before the explosive Edward Snowden/NSA leaks which revealed the pervasiveness – at a global scale – of state mass surveillance abuse, by the 'Five Eyes' – the intelligence services of the US, Canada, the UK, Australia and New Zealand.

He also noted that "the right to privacy can be subject to restrictions or limitations under certain exceptional circumstances. This may include State surveillance measures for the purposes of administration of criminal justice, prevention of crime or combating terrorism".

58. https://www.mediaanddemocracy.com/uploads/1/6/5/7/16577624/sa_surveillancestate-web.pdf
59. The paper can be accessed at: http://ssrn.com/abstract=2239412
60. https://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf

La Rue argued that such interference should only take place if "the criteria for permissible limitations under international human rights law are met". Hence, there should be a law that outlines the conditions whereby individuals' right to privacy can be restricted under exceptional circumstances. "Measures encroaching upon this right must be taken on the basis of a specific decision by a State authority expressly empowered by law to do so, usually the judiciary, for the purpose of protecting the rights of others, for example to secure evidence to prevent the commission of a crime, and must respect the principle of proportionality."

To summarise, by quoting Richards[61] again, it needs to be underscored that: "first, surveillance by government and private actors threatens intellectual privacy and chills the exercise of vital civil liberties; and second, surveillance affects the power balance between individuals and those who are watching, increasing the risk of persuasion, blackmail, and other harmful uses of sensitive information by others."

And finally, "above all, surveillance scholars continually reaffirm that, while surveillance by government and others can have many purposes, a recurrent purpose of surveillance is to control behaviour".

Richards' four principles

In 2013, Neil M. Richards proposed a set of four principles "that should guide the future development of surveillance law, allowing for a more appropriate balance between the costs and benefits of government surveillance".

His four principles are (quoted):

"First, we must recognize that *surveillance transcends the public/private divide.* Public and private surveillance are simply related parts of the same problem, rather than wholly discrete. Even if we are ultimately more concerned with government surveillance, any solution must grapple with the complex relationships between government and corporate watchers.

Second, we must recognize that *secret surveillance is illegitimate* and prohibit the creation of any domestic-surveillance programs whose existence is secret.

Third, we should recognize that *total surveillance is illegitimate* and reject the idea that it is acceptable for the government to record all Internet activity without authorization. Government surveillance of the Internet is a power with the potential for massive abuse. Like its precursor of telephone wiretapping, it must be subjected to meaningful judicial process before it is authorized. We should carefully scrutinize any surveillance that threatens our intellectual privacy.

Fourth, we must recognize that *surveillance is harmful.* Surveillance menaces intellectual privacy and increases the risk of blackmail, coercion, and discrimination; accordingly, we must recognize surveillance as a harm in constitutional standing doctrine. Explaining the harms of surveillance in a doctrinally sensitive way is essential if we want to avoid sacrificing our vital civil liberties."

Source: The Dangers of Surveillance (2013)

61. Under 'Surveillance and Intellectual Privacy' in 'The Dangers of Surveillance'.

NECESSARY & PROPORTIONATE[62]

International Principles on the Application of Human Rights to Communications Surveillance

The 13 Principles:

Legality
Any limitation to human rights must be prescribed by law. The State must not adopt or implement a measure that interferes with these rights in the absence of an existing publicly available legislative act, which meets a standard of clarity and precision that is sufficient to ensure that individuals have advance notice of and can foresee its application.

Legitimate Aim
Laws should only permit Communications Surveillance by specified State authorities to achieve a legitimate aim that corresponds to a predominantly important legal interest that is necessary in a democratic society.

Necessity
Surveillance laws, regulations, activities, powers, or authorities must be limited to those which are strictly and demonstrably necessary to achieve a legitimate aim.

Adequacy
Any instance of Communications Surveillance authorised by law must be appropriate to fulfil the specific Legitimate Aim identified.

Proportionality
Communications surveillance should be regarded as a highly intrusive act that interferes with human rights threatening the foundations of a democratic society. Decisions about Communications Surveillance must consider the sensitivity of the information accessed and the severity of the infringement on human rights and other competing interests.

Competent Judicial Authority
Determinations related to Communications Surveillance must be made by a competent judicial authority that is impartial and independent.

Due Process
Due process requires that States respect and guarantee individuals' human rights by ensuring that lawful procedures that govern any interference with human rights are properly enumerated in law, consistently practiced, and available to the general public.

User Notification
Those whose communications are being surveilled should be notified of a decision authorising Communications Surveillance with enough time and information to enable them to challenge the decision or seek other remedies and should have access to the materials presented in support of the application for authorisation. Delay in notification should only be justified in very specific circumstances.

Transparency
States should be transparent about the use and scope of Communications Surveillance laws, regulations, activities, powers, or authorities.

62. https://necessaryandproportionate.org/files/2016/03/04/en_principles_2014.pdf

Public Oversight
States should establish independent oversight mechanisms to ensure transparency and accountability of Communications Surveillance.

Integrity of Communications and Systems
In order to ensure the integrity, security and privacy of communications systems, and in recognition of the fact that compromising security for State purposes almost always compromises security more generally, States should not compel service providers or hardware or software vendors to build surveillance or monitoring capability into their systems, or to collect or retain particular information purely for State Communications Surveillance purposes.

Safeguards for International Cooperation
In response to changes in the flows of information, and in communications technologies and services, States may need to seek assistance from foreign service providers and States.

Safeguards for Illegitimate Access
States should enact legislation criminalising illegal Communications Surveillance by public or private actors.

6. CONCLUSION

Based on what could be gathered by investigating the records of various sources, it seems clear that Namibia already has formidable and sophisticated communications surveillance capabilities. This is not the concerning part.

What is concerning is that Namibian authorities appear to be using these capabilities despite the primary legal framework – Part 6 of the Communications Act of 2009 – for the deployment of such capabilities not being in force yet (in May 2019).

To be clear, surveillance in itself has positive and negative aspects, but it should be recognised that surveillance is a very uncomfortable concept to contemplate in the context of a rights-based society, and especially as the importance of privacy gains in salience. Nevertheless, surveillance practices, if applied within the frameworks of the law and in the appropriate conditions or circumstances, could be valuable in maintaining safety and security and order and peace.

However, in circumstances where regulatory and oversight mechanisms are weak or lacking, as appears to be the case in Namibia, then surveillance capabilities can very easily be abused. This abuse can have a 'chilling effect' by entrenching fearfulness and self-censorship in society and consequently undermine the still fragile democratic order.

It should be underscored that of significant concern in such circumstances is the invasion and violation of the right to privacy, and equally what effect such an invasion and violation has on the freedoms of speech and association. While most people probably do not mind some level or degree of surveillance, especially where it is meant to and seen to fight crime, the field of surveillance studies seems to be clear that unchecked surveillance powers can lead to an evaporation of trust between states and citizens, as suspicions of surveillance abuse contribute to fuelling socio-political discontent and the undermining of narratives aimed at fostering safety and security, as well as social cohesion.

But the securocratic mindset does not see this, but rather views freedom of expression, access to information and the right to privacy, which all go hand-in-hand, when exercised robustly, as a threat to the social order and 'national security'. This is problematic, for such thinking does not recognise that ultimately transparency is security and that secrecy breeds instability.

As an emerging democracy Namibia still has a long way to go to achieve the robust rule of law and a law-abiding culture. In this discussion, this is reflected in the fact that the security and intelligence apparatus of the Namibian state seems to operate with a sense of impunity and non-accountability.

ABOUT THE AUTHOR

Frederico Links has been an IPPR Research Associate since 2009. He has focussed on democracy and elections, party political finance, empowerment policies, internet governance, cybersecurity and public procurement. He has previously worked as a journalist for a range of Namibian publications. He is the current Chairperson of the ACTION Coalition which campaigns for greater access to information in Namibia.

About Democracy Report

Democracy Report is a project of the IPPR which analyses and disseminates information relating to the legislative agenda of Namibia's Parliament. The project aims to promote public participation in debates concerning the work of Parliament by publishing regular analyses of legislation and other issues before the National Assembly and the National Council. Democracy Report is funded by the Embassy of Finland.

About 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