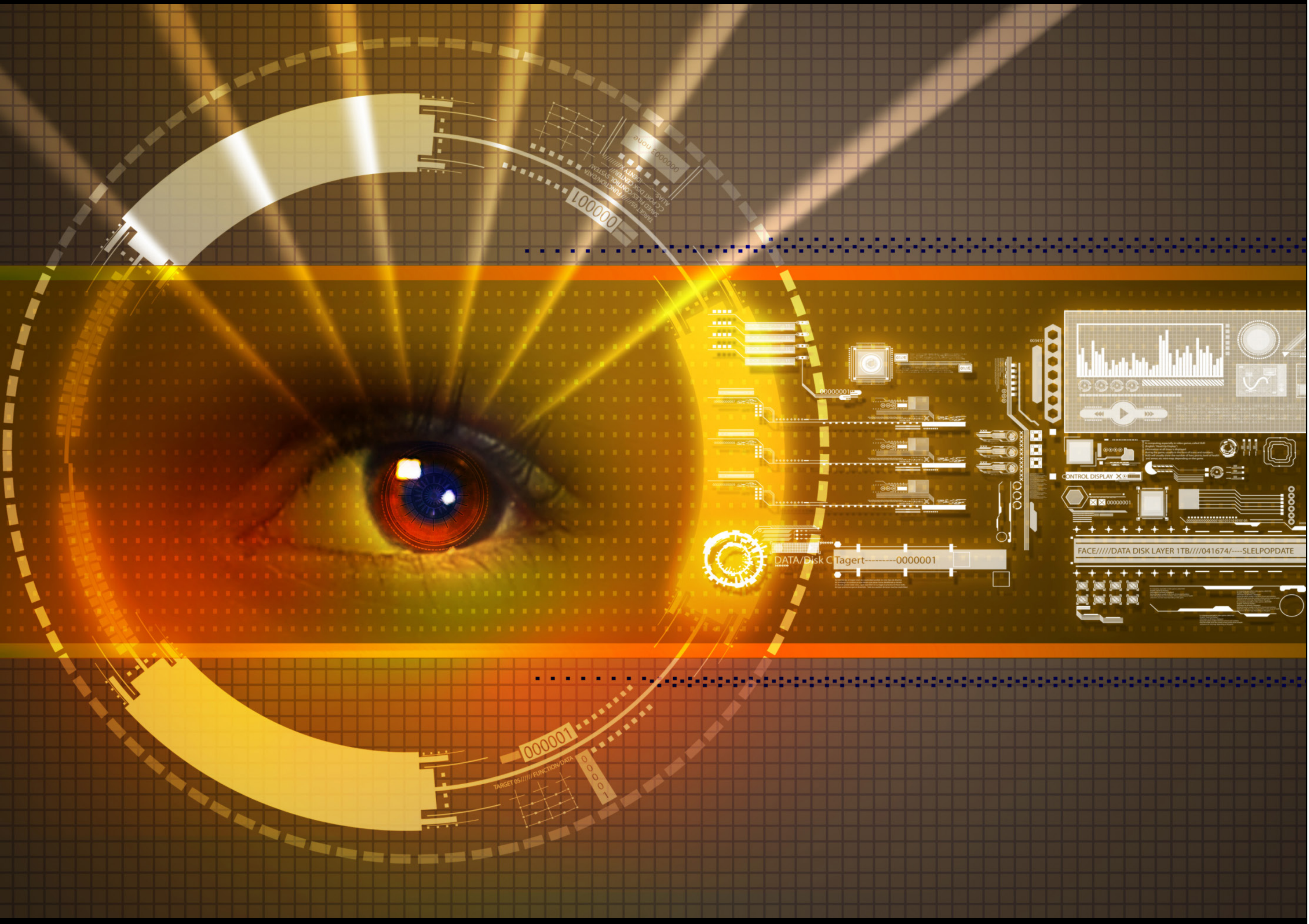
Preliminary Human Rights Defenders' Surveillance perception Report in Uganda, 2016


000001
DATA/Disk C Tagert---------0000001
FACE/////DATA DISK LAYER 1TB////041674/----SLELPOPDATE
CONTROL DISPLAY

Unwanted Witness

Amplifying voices Changing lives

Preliminary Human Rights Defenders' Surveillance perception Report in Uganda, 2016

Unwanted Witness
Amplifying voices Changing lives

Published by:

Unwanted Witness

CITATION:

The Report can be cited as: 'Preliminary Human Rights Defenders' Surveillance perception Report in Uganda, 2016'

Design and layout by:

Esam Concepts (U) Ltd, Tel: 0774438107

TABLE OF CONTENTS

BACKGROUND

Over the last few years, the government in Uganda has implemented a number of legal restrictions on citizen and activist access to and use of online communications. This, coupled with high costs, slow Internet speeds, government surveillance,[1] website blocking and internet shut-downs[2], official crack-downs on cyber communication[3] and the passing of laws to restrict user anonymity and privacy online, has made the citizenry afraid to freely express and share content online[4]. Telecom companies and ISPs are cooperating quietly with government requests to share private user information to the government without going through legal channels.[5]

In 2014, the Uganda police set up the cyber crimes unit, with the intention of fighting cyber crimes, and with help from foreign experts, trained its staff to monitor cybercrimes[6]. This move was criticized by human rights activities as lacking transparency and prone to abuse by self-seekers who may gain access to peoples' private data and communication[7]

Unfortunately, as the government moves to undertake systematic surveillance, the lack of transparency and accountability of these policies and practices means that internet users, including Human Rights Defenders, government critics and online activists, are not aware about the nature of communication surveillance they may be subject to, and are thus ill-equipped to take the necessary measures to protect themselves, their data and communications from unlawful interference.

Objectives of the Study

In order to understand the key operating environment for human rights defenders and activists in Uganda, specifically threats to their online communication and physical arrests and intimidation, Unwanted Witness conducted a series of interviews with 20 purposively selected HRDs and activists. This research is a follow-up to a 2014 study[8] conducted by UW on the state of internet freedoms in Uganda, with a particular focus on HRDs and other online activists.

Among the key issues that the research sought to find out included; level of exposure to risks, threats and attacks; perceptions on government surveillance on their online communication and the tools they are using to circumvent the surveillance; the level of digital security preparedness; the ongoing trends in arrests and detention of HRDs due to their online activism.

The scope of this research was limited to Kampala-based HRDs. Unwanted Witness will be conducting a larger research survey that will seek to engage HRDs across the country.

[1] https://www.privacyinternational.org/node/737

[2] http://cipesa.org/?wpfb_dl=225

[3] http://www.monitor.co.ug/News/National/Crackdown-on-social-media-crime-starts/-/688334/2760414/-/snxsk9/-/index.htm

[4] https://webwewant.org/news/responding_to_digital_security_threats_in_uganda/

[5] https://freedomhouse.org/report/freedom-net/2014/uganda

[6] http://www.monitor.co.ug/News/National/Activists-cry-foul-as-police-set-up-cyber-crime-unit/688334-2249294-r8ixtjz/index.html

[7] http://www.sunrise.ug/news/201507/activists-express-fear-over-the-police-cybercrime-unit.html

[8] https://www.unwantedwitness.or.ug/wp-content/uploads/2014/01/internet-they-are-coming-for-it-too.pdf

STATE OF SURVEILLANCE IN UGANDA

Over the past decade, there has been an increased concern about surveillance of political dissidents, human rights defenders, and journalists in Uganda[9], particularly in response to the government's increased efforts to allegedly address the threats of terrorism.[10]

In 2007, State House brought in a team of Israeli computer experts to coach Uganda's Intelligence security organs on how to; (i) hack into e-mail accounts of individuals perceived to be opponents of government including opposition politicians, human rights activists, journalists and lawyers among others, (ii) carry out forensic investigations on computer hard drives especially those allegedly found in possession of opponents of government and (iii), operate surveillance equipment that monitors both voice and data communications.[11]

In 2010, the government finally enacted the Regulation of Interception of Communications Act, providing for the lawful interception and monitoring of certain communications in the course of their transmission through a telecommunication, postal or any other related service or system in Uganda[12]. The bill had been introduced three years before but was withdrawn after sustained resistance from members of Parliament[13]. The Act has broad provisions for the interception of communications with limited oversight or safeguards. This Act provides for lawful interception and monitoring of communications in the course of their transmission through telecommunications, postal or any other related services or systems in Uganda. Under Section 3, it gives the ICT minister the powers "to set up a monitoring centre, equip, operate and maintain the centre, acquire, install and maintain connections between telecommunication systems and the Monitoring Centre; and administer the Monitoring Centre at the expense of the state."

Section 8 of this Act requires service providers to provide assistance in intercepting communication by ensuring that their telecommunication systems are technically capable of supporting lawful interception at all times. Non-compliance by service providers is punishable by a fine not exceeding UGX2.24 million (US$896) or imprisonment for a period not exceeding five years or both. Non-compliance could also lead to the cancellation of an operator's license.

In addition to the RIC Act, clauses in the 2002 Anti-Terrorism Act give security officers, appointed by the interior minister, the power to intercept communications of individuals suspected of terrorism and to keep them under surveillance, without judicial oversight.[14]

Additionally, the capacity for anonymous communication is being compromised by the mandatory registration of mobile phone SIM cards and mobile internet subscription[15].

[9] https://www.defenddefenders.org/wp-content/uploads/2016/03/The-Right-to-Privacy-in-Uganda-Uganda.pdf

[10] https://freedomhouse.org/sites/default/files/resources/FOTN%202015_Uganda.pdf

[11] https://www.unwantedwitness.or.ug/wp-content/uploads/2014/01/internet-they-are-coming-for-it-too.pdf

[12] http://www.ulii.org/ug/legislation/act/2010/18/Regulations%20of%20Interception%20of%20Communications%20Act%2C%202010.pdf

[13] http://acme-ug.org/2010/07/23/parliament-passes-law-to-intercept-communications-following-uganda-attacks/

[14] https://freedomhouse.org/sites/default/files/resources/FOTN%202015_Uganda.pdf

[15] Ibid

Although the extent of the surveillance capabilities of the Government of Uganda is unclear, a 2015 investigative report by Privacy International (PI) provides evidence of the sale of intrusion malware FinFisher by Gamma International GmbH ('Gamma') to the Ugandan military. The malware was used to infect communications devices of key opposition leaders, media and establishment insiders over period between 2011 and 2013. The secret operation was codenamed Fungua Macho ('open your eyes' in Swahili).[16]

According to the report published by PI, covert FinFisher's access points in form of Local Area Networks (LAN) were installed within Parliament and key government institutions. Actual and suspected government opponents were targeted in their homes. Hotels in Kampala, Entebbe and Masaka were also compromised to facilitate infection of targets' devices.[17] Fake LANs and wireless hotspots were set up in apartment estates and neighbourhoods where many wealthy Ugandans and expatriates live.[18]

The tool chosen as the 'backbone' of the Fungua Macho operation, FinFisher, was intrusion malware at the time manufactured by the Gamma Group of companies, headquartered in the UK. Once infected, a person's computer or phone can be remotely monitored in real time. Activities on the device become visible. Passwords, files, microphones and cameras can be viewed and manipulated without the target's knowledge.[19]

Survey Findings

In presenting these findings, the names of the interviewees have been disguised to protect their identity.

Exposure to security risks, threats and attacks

From the interviews, it is clear that human rights defenders and activists perceive themselves at risk given the number of threats and the possibility of physical attacks on any given day, with not many avenues available for redress. Among the interviewees, all the human rights lawyers felt that they were particularly threatened for their association with certain activists who are perceived as hostile to the government.

"Being an activist lawyer, requires that you must make a deliberate assessment of a spill of the risks that activists face because the risks that activists face often times, spillover to the lawyers. People perceive you to be part and parcel of the problem that your client is involved into. …, in my personal experience, there have been several occasions where my life is put at the same risk as the activists for whom I was working," Says AM, a human rights lawyers working in Kampala.

According to "IS", a human rights lawyer based in Kampala, "there is always an inherent risk in representing clients. If the client's security is compromised or [he or she] is a victim of oppression by the security forces, naturally his/her rescuers are exposed to the same risk."

"…[W]e have the threats and we have been tortured. The challenge we have in Uganda in activism is that we lack support … (and) we don't have where to start in suing the government because all the (government) institutions are (compromised)" notes, "VK", a human rights activist.

[16] https://www.defenddefenders.org/wp-content/uploads/2016/03/The-Right-to-Privacy-in-Uganda-Uganda.pdf

[17] https://www.privacyinternational.org/node/656

[18] Ibid

[19] https://privacyinternational.org/sites/default/files/Uganda_Report.pdf

Even where cases have been instituted against the government, it is always difficult to win due to a lack of evidence. "We lack the necessary cooperation from the state agencies from which we need the evidence, and sometimes we have to facilitate the process, given the fact that most of these cases are not funded and the complainant have no capacity to pay the legal fees"' adds "SM", a human rights lawyer.

Concerning Digital Safety and Security and interception of communication

Besides conventional physical threats, risks and attacks, HRDs and activists are increasingly targeted online for their work[20]. While some have taken some steps to reduce their exposure to these risks and threats as well as mitigate the consequences, the majority do not have the knowledge, skills or the capacity, as well as institutional support to deal with the increasingly sophisticated surveillance and cyber attacks being meted out by the government against HRDs and activists.

Among the key digital threats mentioned by the interviewees included; attempted break-ins to HRDs' email and other social media accounts, interceptions of phone communications, as well spamming and messages of hatred.

According to AM, "there have been several incidents of text notifications from Gmail[21] that somebody has been attempting to log into my account. Secondly, my Twitter handle has received enormous friend requests and followers from people who appear to be sex workers/prostitutes because the pictures on their pages are of their buttocks and things like that and it's suspicious."

"The incidents that have been worrying is that people having meeting with us relying the contents to security personnel. And that has happened by way of tapping into our communications or bugging the rooms where we meet," adds AM.

The majority of the HRDs and activists interviewed reported regular loss of phone reception even in areas known to have good reception, and blockage from sending or receiving text messages. "Sometimes you can hear someone complaining that he is not hearing me because there is always a funny noise in the background," explains VK, an activist.

Where online surveillance has failed, the state has often resorted to physical tactics where computers, laptops and phones of HRDs and activists have been confiscated, or mysteriously stolen from cars, offices, and homes[22].

According to Mr. "OA", a human rights activist, the interception of communication is "so frequent, especially when the government suspects that there will be a demonstration of any time, our phone communication are intercepted. It is possible to call me and hear a lot of background noise as if I am in the market yet I am seated in the house," he explains.

[20] http://www.hrcug.org/publications/file/Human%20Rights%20Defenders%20in%20Uganda%20M.pdf

[21] Google has this notification for suspected state-sponsored attacks https://security.googleblog.com/2012/06/security-warnings-for-suspected-state.html

[22] http://www.hrcug.org/publications/file/Human%20Rights%20Defenders%20in%20Uganda%20M.pdf

"In as far as the actual content of the communications between people over phone is a concern, but that hasn't been the case. What has been the case is that the identity of the person you have been speaking to. They will ask you why you have been talking to so and so on skype yesterday. You are just the two of you on Skype, but they know that you spoke. So, quite evidently, they have a backup access to at least know the people you call and can see that you spoke.

In terms of the content, we have not been encountered by the incidents where they will tell you the content. But on several occasions, you are confronted with the name of the person and the time you spoke to and how long," explains SM

There is a general agreement among HRDs that it is impossible to beat the risks. "We can only mitigate and minimize it. …also, the nature of the risks keep changing. Sometimes we are not well versed with what the new risks are. So, our risks continue being vulnerable." Explains SM

Risks and threats to HRDs are also heightened by the people work around them, especially when the team does not adhere and implement the organisation's safety and protection protocols/policies, as is explained by AM, a human rights lawyer. "…you will say as a policy that don't use personal laptops to carry sensitive work for organization or don't use personal laptops to communicate official communications because office computers have security systems. However, people will also go against this policy and expose the rest of the team of sensitive documents to cyber attacks and interceptions,"

Also, as a coping mechanism, human right lawyers reporting encouraging the people they work with to use non-electronic communication when communicating with human rights activists since most of them are not sophisticated and have no idea about safety.

Tools used for protection online

HRDs and activists have adopted a number of tools to aid them reduce their exposure to risks and threats including online surveillance and protect their online communication, as well as mitigate the related consequences. Among the tools used by the HRDs, include double layer security systems; encryption; Virtual Private Network (VPN), Vismo, which is a GPS tracking application designed to locate individuals travelling the world using their smartphone, tablet or personal GPS Trackers[23] among others.

"I have a double layer security system on my Gmail account. The advantage with this is that each time someone is trying to enter into your account, Gmail sends you a text information; and I have paid VPN that is running on all my gadgets all the time to protect my gadgets from surveillance," explains AM.

Additionally, there have been a number of capacity building initiatives aimed at equipping the HRDs and activists with the necessary tools, knowledge and skills to enhance their online safety.

In January 2014, Unwanted Witness, with support from the Web We Want held a workshop for online activists in Uganda, which brought together 10 activists who use the Internet as platforms of expression.[24]

[23] http://www.vismo.com/

[24] https://webwewant.org/news/responding_to_digital_security_threats_in_uganda/

However, it is clear from the interviews that majority of HRDs and activists have limited knowledge, skills and access to the tools that will enhance the safeguard their online communication, especially encryption tools, despite being aware that their communication is being monitored.
"I am aware that they tap our phones, but of course as someone who is not an expert in computer or IT (Information and Communication Technologies), I haven't gotten the skills so far to curb the problem," confesses NT, an activist.

Given the fact that technology is always changing and governments are also increasingly becoming more sophisticated, it is important that HRDs and online activists continuously update review their vulnerabilities and update their hardware and software on a regular basis and adopt smart multilayered security and protection systems.

Arrest and detention of HRDs and activists for their online activities

The arrest and detention of HRDs and activists in Uganda due to their online activism has been on the rise. In June 2015 Robert Shaka, who frequently posts views critical of the government on social media was arrested and detained by the police for "offensive communication." The government alleges that Shaka, an information and security analyst, violated the Computer Use Act by posting statements about the president's health status.[25]

In January 2016, another government social media critic, Charles Rwomushana was arrested and detained by police on suspicion of circulating photographs of missing Christopher Aine's 'dead body' on social media.[26]

In the majority of the arrests, the authorities' intentions are not very clear as only Robert Shaka was charged and taken to court for prosecution. The rest have been detained and later released on Police bond. According to AM, the police's goal is to retrieve passwords and see what is on your phone, "…but the arrests have … primarily intended not to prosecute but rather intimidate online activists."

Shaka was abducted in the early hours of the morning. Upon his arrest by the police, the first thing they did was to confiscate all of his phones and computers, including flash disks at his home, according to his lawyer, Mr. Nicholas Opiyo.

Need for Capacity building in Digital Security

From the interviews, it is clear that HRDs and activists continue to engage in insecure and un- encrypted online communication, thus exposing themselves, their associates and personal communications to government surveillance. The majority express a lack of knowledge and skills to secure online communication, including basic encryption.

This is despite the number of initiatives that have been undertaken by key players such as Defenders Protection Initiative, ARTICLE 19, Human Rights Network for Journalists – Uganda, among others to build the skills of HRDs in secure online communication. It is therefore important that more training opportunities are provided for HRDs and other activists to enhance the security of their online activism.

[25] http://www.voanews.com/a/social-media-critic-arrested-in-uganda-/2820626.html
[26] http://ntv.co.ug/news/crime/09/jan/2016/charles-rwomushana-arrested-over-aine-pictures-10675

CONCLUSIONS

Surveillance against HRDs and activists in Uganda has had a chilling effect on free speech, legitimate expression of political dissent as well as other fundamental human rights. There is a lack of transparency, accountability and clarity in the policies and practices employed by the state in their fight against cyber terrorism and in the end, critical voices against the government have become the target.

The use of provision of retrogressive laws, such as the Anti-Terrorism Act (2002), Computer Misuse Act (2011), and others that give broad powers to the interception of communications and surveillance without judicial oversight greatly impacts on people's enjoyment of their right to privacy.

The threats to human rights lawyers purely for their association with individuals with perceived contrary views to those of the state greatly undermines peoples' right to a fair hearing and legal representation. This is because fewer lawyers are now willing to provide legal representation to perceived government enemies.

RECOMMENDATIONS

To the Government

The government should amend retrogressive laws and policies, such as the Regulations of Interception of Communications Act 2010, the Computer Misuse Act 2011 and the Anti-Terrorism Act 2002, that give broad powers for the interception of communication and surveillance, because these are open to abuse. The government should expedite the passage of the Privacy and Data Protection Bill to guarantee the right to peoples' privacy of their data.

CSOs

Civil society working with HRDs, including the media should advocate and demand for the repeal and annulment of retrogressive laws and policies that legalise online surveillance and interception of communication

Civil society should also seek to empower HRDs and online activists with the necessary tools, knowledge and skills to reduce their vulnerability to online risks and threats due to their nature of work

HRDs and Activists

At all times, HRDs and online activists should empower themselves with the requisite skills, knowledge and tools that will enable them reduce their vulnerabilities by adopting smart and multi-layered security systems

Plot 41 Gaddafi Road
P.O.Box 71314 Clock Tower K'la

Tel: +256 414 697 635
Email: info@unwantedwitness.or.ug
www.unwantedwitness.or.ug
Unwantedwitness-Uganda
@unwantedwitness
unwantedwitness