East African
Communications
Organisation

Communications for all in East Africa

CURBING THE COMMUNICATIONS INFRASTRUCTURE VANDALISM VICE IN THE EAST AFRICAN COMMUNITY

Prepared by EACO
JULY 2018

TABLE OF CONTENTS

1   INTRODUCTION

Information and knowledge have been regarded as the basic factors for development. Information communication technologies therefore provide an avenue for the exchange of such information and knowledge. Developing countries and in particular, the East African nations, face an uphill task raising the huge resources needed to develop communications infrastructure that can be used as a launch pad for economic development.

Yet, there are many cases reported across the region of vandalism of the communications infrastructure, which increases cost of communication and also scares away potential investors into the region. On the background of the high prevalence of the communication infrastructure vandalism that a paper has been prepared, detailing the causes, effect and proposed solutions to the vice.

2   PROBLEM STATEMENT

While communication services remain central to the economic development of countries over the world, a major setback to the providers of services remains vandalism. This has led to significant financial losses to the owners of the vandalised equipment and also led to the degradation of communication services.

3   METHODOLOGY

In order to appreciate the extent of the problem of vandalism and the possible long lasting solutions, a structured questionnaire was formulated and shared with the different regulators in the East African community who in turn shared the same with the operators in the respective countries. The responses received together with the review of different literature were used in coming up with this report.

4   CAUSES OF VANDALISM

The high demand for various infrastructure components such as batteries, diesel, and copper encourage vandals to get involved in this trade. Vandalism forms include the siphoning of fuel from the generators, stealing of back-up batteries and lightening arrestors, fibre cable cuts (deliberate or otherwise), solar panels, stealing of copper rods from masts.

In certain cases, communications infrastructure is vandalised accidentally. This most happens during excavations and road repairs and constructions especially in the urban areas.

From the responses received from the operators, the following were indicated as the causes of vandalism;

a. Unemployment (economic)

There is an indication that because of the widespread poverty caused by unemployment, some people especially the youth decide to steal parts of the communication infrastructure for sale as a means of earning their livelihood. To them, the cost to the network due to their actions is far less than the benefit realised from the proceeds of the sale.

b. Demand for diesel, batteries and copper

There is a high demand for diesel, batteries and copper. The possibility of getting all these at no or less cost has lured many into vandalising the different equipment at different installations since there is ready market for them.

c. Sabotage (anti-competitive)

It has also been indicated that there is sabotage by the rival operators such as intentional cutting of fibre/cables. This is in order to degrade the quality of service of competitors which is an extreme case of anti- competitive behaviour.

d. Ignorance (lack of awareness)

There also instances where vandalism has been attributed to ignorance. At times, the persons who destroy the infrastructure do not have an idea about how important the equipment maybe.

e. Insecurity (political)

In countries with cases of insecurity on unrest, communication infrastructure becomes collateral damage. The people involved just vent anger at any facilities and in a number of cases, these has been communication infrastructure. Such has been the case where people for one reason or the other are demonstrating against government.

f. Accidental Damage

Various activities such as road and building construction have led to damage of facilities such as underground cables. Although this is unintended, the responded indicated that there is a major occurrence of this type of damage to their installations.

5   EFFECTS OF VANDALISM

From the received responses, vandalism has had various effects on the operators as well as the consumers of services;

a. Cost to the communication companies:

The monetary cost to the communication companies is huge. In Uganda, two telecom companies lost a total of 100,000 litres of fuel and 200 batteries in a single year. In Tanzania, one of the telecom operators indicated that they lost a total of USD 340,000 in 2015 while it is estimated that Kenya loses between KShs1.5 billion and KShs 2 billion per year in vandalism.

Vandalism increases the operational and maintenance costs and the re-investment costs. This inevitably leads to reduced revenue margins, which can only be prevented by increasing in the pricing of the communication services.

Act of Vandalism was identified also in Burundi by telecoms operators and it cost a lot of money. In 2016, it was estimated that only VIETTEL Telecoms Company loses between 5 hundred thousand to 2 million BIF per year in vandalism.

b. Service Quality

Vandalism has a negative impact on the quality of service. It is inevitable for the consumers to experience poor communication services once there is damage to fibre or once fuel has been siphoned from generators, batteries stolen or towers vandalised. Consumers are denied the chance to enjoy a service level quality commensurate with what they pay for.

c. Hindrance to Investment

Vandalism scares away prospective investors. Communication infrastructure is an expensive to invest in. With high possibilities of the installed infrastructure being destroyed, it is probable that any serious investor will hesitate to invest in such an economy.

6   LEGAL PROVISIONS AGAINST VANDALISM IN THE EAST AFRICAN STATES

In order to appreciate the extent to which vandalism has been provided for in the laws of the different countries within the East African Community, the respective acts regarding communication and penal codes were scrutinised

6.1   Uganda

Section 83 of the Uganda Communications Act provides for the protection of the telecommunication installations and the implications for any person who damages or tampers with a telecommunication installation.

Section 83 (1)(b): A person who damages, removes or tampers with any installation or plant or any part of it belonging to an operator, commits an offence and is liable on conviction to a fine not exceeding one hundred and twenty currency points or imprisonment not exceeding five years or both and on a subsequent conviction to a fine not exceeding two hundred and forty currency points or imprisonment not exceeding ten years or both.

The provision appears adequate and if enforced would probably deter or minimise cases of vandalising the communication infrastructure. It would therefore appear that in Uganda's case, the challenge would not be lack of stringent punitive measures provided for in the law, but something else.

6.2   Kenya

Section 32 of the Communications Act of Kenya states that**:** *A person who wilfully, with intent to unlawfully intercept or acquaint himself or herself with the contents of any message; vandalizes, damages, removes, tampers with, touches or in any other way whatsoever interferes with any telecommunication apparatus or telecommunication line, post, or anything whatsoever, being part of or used in or about any licensed telecommunication system, commits an offence and shall be liable, on conviction to a fine of not less than five million shillings or to imprisonment for a term of not less than ten years or to both.*

The Kenyan communication law also has adequate provisions against vandalism in the sector.

6.3   Rwanda

While Rwanda's Communications Act does not provide for measures against vandalism, the Penal Code adequately makes a provision for vandalism against any type of infrastructure be it communication or not**.** Article 406 of the Penal Code States that: *Any person who wilfully destroys or damages in any way, in all or a part, buildings, bridges, dams, water pipes, water pipe routes, roads, railways or any other means of communication or electric power infrastructure, wells or any other buildings which do not belong to him/her, shall be liable to a term of imprisonment of two (2) years to five (5) years and a fine of twice (2) to ten (10) times the value of the damaged property.*

6.4   Tanzania

The section 151 (1) of the Electronic and Postal Communications Act (EPOCA) 2010, states that: *any person who wilfully removes, destroy or damages any installation or plant used for postal or Electronic communication services commits an offence and shall be liable on*

conviction to a fine not less than one million shillings or to imprisonment for a term not less than three years or to both.

6.5 Burundi

The Burundi Penal Code, article 322 adequately makes a provision for vandalism against any type of infrastructure be it communication or not. This article of the Penal Code States that: "*Any person who wilfully destroys or damages in any way, in all or a part, buildings, bridges, dams, water pipes, routes, roads, railways or any other means of communication or electric power infrastructure, wells or any other buildings which do not belong to him/her, shall be liable to a term of imprisonment of one (1) month to five (5) years and will also pay an amende 10.000 to 100.000 BIF.''*

7 ADDRESSING THE VANDALISM CHALLENGE

7.1 Restrictions on Access to Infrastructure Sites

From the interaction with the operators, there are cases of vandalism that have been reported resulting laxity in restrictions to the facility. To avoid such, there should be access control procedures. This must entail how one accesses the sites, who is supposed to authorise entry to the facility, how confirmation should be made by the persons securing the facility. By having such measures in place, it becomes harder for any criminal minded persons especially the former employees of the companies to dupe the security at the installations into giving them access.

7.2 Certification

There is need for the regulatory agencies to certify technical personnel (**Kenya is already doing so**). No technical employee of any company involved in communications infrastructure services should be allowed to perform any technical duties before certification. Certification of staff will enable the creation of an authorized persons' database to support staff recruitment (consulting database of certified personnel) and where applicable upon misconduct, such certification be revoked and individual delisted/blacklisted. This will minimize hire of unsuitable individuals by all operators as well as discourage destruction of communications equipment.

7.3 Protection of Batteries

From the responses received from the various operators, theft of the batteries is very prevalent. In fact, two Ugandan companies lost 200 site back up batteries in a particular year, yet batteries are an important communication component.

In order to minimise incidences of them of batteries, there should be labelling of the batteries for ease of identification, so that the buyers can easily be traced to the origin. This can make theft of batteries less lucrative.

A consideration should also be made by companies to ensure that the batteries are GPS enabled to facilitate easy monitoring and appropriate reaction.

7.4 Data/information sharing

There is also need to create a consolidated database of activities and installations. Such a database of stakeholder activities (who is doing what, where and when) should be regularly updated and regular activity reports should be shared with all stakeholders. This would help in identifying and alerting other operators on new forms of vandalism and how such would be managed.

7.5 Collaboration with Police

By the nature of the activity, there is a requirement for the different companies to have a working understanding with the security agencies like the police. Such an understanding makes it much easier to investigate and pursue such cases leading to prosecution and possible conviction of the culprits. A memorandum of understanding between operators on one hand and the police on the other can focus on;

- Procedures for reporting cases and management of evidence
- Site security systems monitoring guidelines
- Setting up a dedicated desk for communications infrastructure at police headquarters.
- Strategies of identifying outlets/shops of stolen equipment
- Dealing with industry practitioners identified as accomplices in vandalism of communications infrastructure.

7.6 Stakeholder Engagement

Plans should be devised to sensitise the public on the dangers vandalism of the communication equipment. Such plans require a coordinated approach by all operators to;

- Educate local communities in the vicinity of sites to increase vigilance
- Identification of consumers of vandalized products
- Work with users of the vandalised equipment e.g. steel industries that use scrap as input
- Destruction of communication infrastructure during works
- Identifying outlets/shops of stolen equipment
- Identification of consumers of vandalized products
- Collaboration between operators, NRAs and the Police
- Formation of vigilante groups within the community- crime preventers

7.7 Naming and Shaming

There is need to discourage the vice, by naming and shaming of those caught in the act. Such actions can deter the others from getting involved in destruction of infrastructure. This must however be done with caution, in order to avoid the possibility of litigation by the affected persons.

7.8 Addressing the unemployment question

Governments need to pay particular attention to the unemployment challenges especially for the youth. Without means of a livelihood, vandalism might still be viewed as a source of income for a number of persons, the risks involved notwithstanding.

7.9 Amendment of laws on destruction and vandalism of Infrastructure

While some of the EAC states have laws and regulations that provide for stringent measures against vandals, others do not. It is therefore important to put in place or strengthen laws dealing destruction or theft of infrastructure components.

It was also observed that a number of countries' laws are specific to communication infrastructure. While this is welcome, there is need to look at addressing the infrastructure problem in a holistic way (Rwanda does), so that laws such as the penal code has prescriptions for punishments against the vice irrespective of the type of infrastructure. With such an approach, it would be easier for the police and prosecution and the judiciary to handle such cases.

8 CONCLUSION

Infrastructure vandalism remains one of the biggest challenges faced by the communication companies, leading to disruption of services to the clients, huge losses in terms of expenditure of operational and maintenance costs as well as reinvestment. There is need therefore for concerted efforts between the NRAs, the operators and other arms of government towards the minimisation or eradication of the vandalism in the communication sector.