This presentation will focus on analysing a case study from Uganda as derived from the United Nations Office on Drugs and Crime (UNODC) database (Sherloc, N.D.). Since the database lacks cybercrime reports from my home country, Kenya, I opted to lean towards Uganda due to it been a neighbouring country and it had more interesting cybercrime cases as compared to Rwanda like the use of electronic evidence in a case, etc. This analysis will provide an examination to the nature of cybercrime in Uganda, how the country is dealing with it, and the public's perception of cybercrime.

The cybercrime chosen is the case of Gachev & Ors v Uganda (Criminal Appeal 155 of 2013) [2016] UGHCCRD 4 (16 July 2016), which is about the four Bulgarian nationals who were charged with forging ATM cards so as to gain unauthorised access to data (Sherloc, N.D.). The reason for choosing this cybercrime is because ATM forgery is one of the major problems combatted in the banking and financial industry in not only Uganda but also globally. This is evident from the fact that the UNODC database contains several similar cases of ATM fraud from different countries, such as:

- Case BGH, Beschluss vom 06.07.2010, 4 StR 555/09 from Germany whereby in February 2017, the defendant created an organized criminal group to produce false payment cards that they would use to withdraw money from ATMs abroad. They used a method called skimming, whereby card readers were used to get data that was necessary to falsify payment cards and a separate storage medium to obtain the PIN.
- A joint operation called “Operation Imperium” was conducted by law enforcement agencies from Bulgaria, Spain and Europol’s European Cybercrime Centre. As a

result, 31 members of an organised criminal group were arrested due to their involvement in ATM skimming, electronic payment fraud, forgery of documents, etc. Moreover, eight criminal labs and the seizure of more than 1,000 devices, including skimming devices, micro camera bars, card readers, magnetic strip readers and writers, computers, phones, flash drives, plastic cards ready to be encoded, 3D printers, and forged credit cards, - were also discovered after 40 houses were searched.

The cybercrime case from Uganda involves an organised criminal group of four Bulgarians who allegedly used a skimming device in the ATM machine to steal information from victims. This ATM skimmer included an ATM card reader and a pinhole camera that they would use a masking tape to fix them on the ATM. A microchip and a phone battery were then used to illegally gain access to bank accounts. Afterwards, they would pick out the bank accounts that held higher sums of money and forge ATM cards to withdraw the money from the account. They would then change the money into dollars and wire it back to their bank accounts in Bulgaria.

This type of crime is known as ATM card forgery or fraud due to the stealing of banking information and counterfeiting ATM cards so as to gain unauthorized access to bank information to make unauthorized payments or money transfers or money withdrawals from the victims (N26, 2023).

Such acts were and are still considered to be against the Confidentiality, Integrity and Availability of computer, data, networks and systems because unauthorised access to

computer systems, data, networks and breach of privacy/data protection measures were achieved.

Uganda's ways of dealing with unauthorised access of computer data is by using its legal framework to prosecute and convict the offenders. Like in the Gachev & Ors v Uganda case, the four Bulgarians nationals were each charged with 33 counts of forgery, one count of conspiracy to commit felony, and one count of unauthorized access of computer data without authority. Furthermore, use of electronic evidence, including the examination of the ATM machines and the analysis of the cloned cards, facilitated the prosecution of the defendants. Uganda has implemented legislation to combat cybercrime, such as the Computer Misuse Act, the Electronic Signatures Act, - which criminalizes unauthorized access to computer systems and networks (Sherloc, N.D.). Moreover, Uganda also collaborated with international organizations such as the International Telecommunication Union to develop strategies for combating cybercrime.

As from the Gachev & Ors v Uganda case report on the UONDC database, information on the costs of the unauthorized access of computer data without authority in Uganda or how it affects effective investigation was not available. However, the victims who their bank accounts had been illegally withdrawn from, were affected and it is not mentioned the cost of the damages or if the victims were compensated or not. The use of electronic evidence in the Gachev & Ors v Uganda case shows that technology can be implemented to effectively investigate and prosecute cybercrime.

The issues concerning the crime investigation while focusing on gathering of evidence includes:

- The use of electronic evidence in the Gachev & Ors v Uganda case shows how technology is significant when conducting a cybercrime investigation and prosecuting of the accused or offender. However, effectiveness of the investigation can be hindered due to it been challenging for the court to accept and rely on the electronic evidence especially if the said evidence is gathered illegally or violated the rights of the offender.
- If the offender is using techniques to hide their activities like encryption, use of VPNs, fake identities, etc, - gathering of electronic evidence might be challenging.
- Education and training for example the need for user awareness to cybercrime risks, cyberlaws, (Anon, 2013)
- The report did not mention if the money that was illegally withdrawn from the account was recovered or not. Therefore, it might have been difficult to trace the digital footprints to the accounts in Bulgaria due to the different legal acts and laws between Bulgaria and Uganda.

Since not a lot of Ugandans are aware of cybercrime risks, their public and social perceptions is low. In addition to that, there is low reporting rate due to lack of

awareness of the legal framework dealing with cybercrimes and public ignorance to cyberlaws and cybercrime risks (Anon, 2013).

Due to lack of awareness, training and education on cybercrime risks and the fast rate at which technology is evolving and been complex, Uganda and most of other countries lack the right tools and skills needed to investigate cybercrimes (Anon, 2013). Additionally, most Ugandans and other developing countries believe that cybercrimes do not target them and is only an issue faced by developed countries. This increases the rate of people and countries not enforcing themselves through education, training and awareness, thus resulting to cybercrimes not been taken seriously or combatted fully, effectively and swiftly.

To conclude, the cybercrime case of Gachev & Ors v Uganda shows how significant electronic evidence is in combating cybercrime like the implementation of CCTV cameras in ATM. Uganda also deals with cybercrime by implementing legislation and other tools, but it can be challenging with how effective it is to investigate and prosecute such crimes.

References

Anon, 2013. *Challenges of Implementing Cyber laws in Uganda.* [Online]
Available at: https://www.summitcl.com/wp-content/uploads/2017/01/Challenges-of-Implementing-Cyber-laws-in-Uganda.pdf
[Accessed 16 April 2023].

N26, 2023. *Debit card fraud—what you need to know.* [Online]
Available at: https://n26.com/en-eu/blog/debit-card-fraud
[Accessed 14 April 2023].

Sherloc, N.D.. *Case Law Database.* [Online]
Available at: https://sherloc.unodc.org/cld//case-law-doc/cybercrimecrimetype/uga/2015/gachev_ors_v_uganda_criminal_appeal_155_of_2013_2016_ughcc

rd_4_16_july_2016.html?lng=en&tmpl=sherloc
[Accessed 11 April 2023].

Sherloc, N.D.. *Case Law Database.* [Online]
Available at:
https://sherloc.unodc.org/cld//v3/sherloc/cldb/search.html?lng=en#?c=%7B%22filters%22:%5B%7B%22fieldName%22:%22en%23__el.caseLaw.crimeTypes_s%22,%22value%22:%22Cybercrime%22%7D%5D,%22sortings%22:%22%22%7D
[Accessed 11 April 2023].

Sherloc, N.D.. *Database of Legislation.* [Online]
Available at:
https://sherloc.unodc.org/cld/v3/sherloc/legdb/search.html?lng=en#?c=%7B%22filters%22:%5B%7B%22fieldName%22:%22en%23__el.legislation.crimeTypes_s%22,%22value%22:%22Cybercrime%22%7D,%7B%22fieldName%22:%22en%23legislation@country_label_s%22,%22value%22:%22U
[Accessed 14 April 2023].