CyberX 2021

# Cybersecurity, Law & Deterrence: Lessons for law enforcement communities

CENTER FOR STRATEGIC AND DEFENCE STUDIES, AFRICA


SECURITY GOVERNANCE INITIATIVE SECRETARIAT

# CyberX Partners

## CENTER FOR STRATEGIC AND DEFENCE STUDIES, AFRICA

CSDS AFRICA provides advanced training and research to government agencies and transnational organizations to improve cybersecurity, maritime and border governance in Africa. - CSDS routinely builds teams to solve Africa's pressing problems.
Join the CSDS AFRICA'S Roll of Experts today.

## SECURITY GOVERNANCE INITIATIVE (SGI) SECRETARIAT

SGI SECRETARIAT is a Department of the Ministry of National Security concerned with cyber, maritime and border security . SGI has led the drafting of Ghana's Cyber, Maritime and Border Strategies since 2017

CYBERX is a regional conference hosted by CSDS AFRICA that addresses the most pertinent issues in cybersecurity today. CyberX focuses on policy issues surrounding cybercrime, strategy and law

CYBERX SPEAKERS

**JIBRIL M RICHTER.**
Policy Analyst and Research Fellow
Center for Strategic and Defence Studies, Africa.

**OSEI BONSU DICKSON, ESQ.**
Director, Legal
Ministry of National Security
Coordinator, Security Governance Initiative

Expertise: Cybersecurity, Cyberlaw and Policy

# GLOBAL CYBERCRIME SITUATION

# AFRICA - CYBERCRIME SITUATION

- Cybercrime costs Africa approximately €3.5bn compared to €528bn worldwide. More than 85% of African financial institutions reported they have already fallen victim to at least one cyberattack resulting in losses, and some faced recurrent attacks.
- 30% involved bank card fraud, while one-third involved phishing, i.e., emails sent with the intention of tricking people into divulging their personal information.
- The third most common target of cyberattacks, accounting for 24% of all cases, is core banking, meaning viruses and intrusions affecting information systems. In addition, African banks are impacted by information leakage, identity theft, money transfer fraud and fake check scams.
- Almost half of the 10 million graduates from more than 668 African universities each year do not find jobs. According to INTERPOL 50% of the cybercriminals that they identified in the region are unemployed.

# GHANA - CYBERCRIME SITUATION

- A 2013 report by the FBI ranked Ghana as the second largest source of cyber fraud and financial scams in Africa

- Ghana lost $50 million to cyber attacks in 2016 while Africa, as a whole, lost $2 billion to cyber-attacks in the same year. Between 2016 and 2018, the country lost over US$200 million to recorded cyber crime cases. According to the Ghana Police Service, more than half of these reported cases were linked to fraud.

- Ghana Police also recorded an increase in cyber crime in the country from 116 in 2016 to 412 in 2017 and further to **558 in 2018**. Ghana has so far recorded a total of 11,550 CASES of cybercrime since launching its Cybercrime Incident Reporting Points of Contact (PoC) in October 2019.This, according to the National Cybersecurity Advisor has been achieved as a result of the National Computer Emergency Response Team (CERT) and the PoC.

# Cybercrime Cases: what you need to know.

# Cybercrime Cases: The Morris Worm (1988)

- The Morris worm or Internet worm was one of the first computer worms distributed via the Internet, and the first to gain significant mainstream media attention.
- Written by a graduate student at Cornell University, **Robert Tappan Morris**, and launched on November 2, 1988, from the computer systems of the Massachusetts Institute of Technology.
- Though Morris **did not intend** for the worm to be actively destructive, instead seeking to merely highlight the weaknesses present in many networks of the time, an unintentional consequence of Morris' coding resulted in the worm being more damaging and easily spread than originally planned.
- Morris was tried and convicted of violating United States Code: Title 18 (18 U.S.C. § 1030), the Computer Fraud and Abuse Act in United States v. Morris. After appeals, he was sentenced to three years' probation, 400 hours of community service, and a fine of $10,050 plus the costs of his supervision. The total fine ran to $13,326, which included a $10,000 fine, $50 special assessment, and $3,276 cost of probation oversight.

# Cybercrime case: Mafiaboy

- On February 7, 2000, Calce, then 15 years old targeted Yahoo! with a project he named Rivolta.
- Rivolta was a distributed-denial-of-service attack which overloaded servers with different types of communications to the point where they became unresponsive to commands. At the time, Yahoo! was a multibillion-dollar web company and the top search engine. Mafiaboy's Rivolta managed to shut down Yahoo! for almost an hour.
- Calce's goal was to establish dominance for himself and TNT, his cybergroup, in the cyberworld. Buy.com was shut down in response. Calce brought down eBay, CNN, and Amazon via DDoS over the next week. Calce attempted but was unsuccessful in bringing down Dell during this DDoS attack. The FBI and the Royal Canadian Mounted Police first noticed Calce when he started claiming in **Internet Relay Chatrooms** that he was responsible for the attacks. He became the chief suspect when he claimed to have brought down Dell's website, an attack that had not been publicized at that time.
- Calce initially denied responsibility but later pleaded guilty to most of the charges brought against him. The Montreal Youth Court sentenced him on September 12, 2001, to eight months of "open custody," one year of probation, restricted use of the Internet, and a small fine.

# Cybercrime Cases: Jonathan James hacks NASA and US Defense Department

- In 1999. Jonathan James was 15 when he penetrated the computers of a US Department of Defense division and installed a ‘backdoor’ on its servers. This allowed him to intercept thousands of internal emails from different government organizations including ones containing usernames and passwords for various military computers.
- James was able to steal a piece of NASA software which cost the space exploration agency $41,000 as systems were shut down for three weeks.
- However, his intrusion into the computers of the Defense Threat Reduction Agency (DTRA), brought him to the attention of the Federal authorities. James later admitted to authorities that he had installed an unauthorized backdoor in a computer server in Dulles, Virginia, which he used to install a sniffer that allowed him to intercept over three thousand messages passing to and from DTRA employees, along with numerous usernames and passwords of other DTRA employees, including at least 10 on official military computers.
- He received a light sentence due to his young age.He committed suicide in 2008 after he was accused of conspiring with other hackers to steal credit card information. James denied the allegation in his suicide letter.

# Cybercrime Cases: Shadow Kill Hackers and Johannesburg City

- A hacker group with the name Shadow Kill Hackers used ransomware to hold South Africa's largest city ransom
- The group demanded 4 bitcoins from Johannesburg authorities, or they'd upload stolen city data on the internet.
- The message was discovered on city employee computers, in the form of a logon screen. The City had to shut down for 24 hours and meant that customers would not be able to transact on e-services or log queries at the call center.
- The hackers went to Twitter to post screenshots showing that they had access to the city's Active Directory server, even claiming that they were the ones who took down the website after deactivating the DNS server. The hackers are still in the wind.

# Cybercrime cases: the TMT Gang

- The TMT gang distribute malware, do phishing campaigns and business email compromise scams affecting about 500,000 companies around the world.
- Three alleged members of the prolific Nigerian cybercrime ring were arrested in Lagos.
- They were brought in after an investigation by Singapore-based cybersecurity firm Group-IB, Interpol and the Nigerian police force. The suspects are alleged to have used phishing links and mass emailing campaigns under the guise of purchasing orders, product inquiries and even Covid-19 aid, infecting organizations and siphoning funds from businesses and individuals.
- The group is believed to have compromised government and private sector companies in more than 150 countries since 2017, including the U.S., Japan, and the U.K. The data discovered on their devices confirmed their involvement in the criminal scheme and identified stolen data from at least 50,000 targeted victims, according to Nigerian police.

# Cybercrime cases: Daniel Kaye and Lonestar

- An attacker by name Daniel Kaye, a Briton was hired and paid $10,000 a month to use his hacking skills to disrupt Lonestar's, an ISP, services and reputation.
- The attacker was hired by a senior employee at Cellcom, an industry competitor of Lonestar, however, it is not clear whether Cellcom was aware of the transaction.
- In October 2015, Daniel Kaye launched series of attacks on Lonestar, which became so powerful that it disrupted the company's internet services the following year. Kaye used Botnet he had created to trigger repeated distributed denial of service requests on botnet while in Cyprus.
- In late February 2017, UK police arrested Kaye at a London airport. Before his prosecution in the UK, authorities first sent him to Germany where he eventually pleaded guilty in July 2017 and received a suspended prison sentence for attacks on Deutche Telekom's network. He was sent back to the UK, where he pleaded guilty for the attacks on Lonestar.

# Maxwell Atugba Abayeta and Others

- Maxwell Atugba Abayeta, located in Tamale and others conspired to commit wire fraud, committed wire fraud, conspired to commit money laundering, conspired to commit computer fraud and aggravated identity theft.
- It is alleged that various Africa-based co-conspirators committed or caused to be committed, a series of intrusions into the servers and email systems of a Memphis-based real estate company in June and July 2016.
- The suspects used sophisticated anonymization techniques, including spoofed email addresses, Virtual Private Networks to identify large financial transactions, initiated fraudulent email correspondence with relevant business parties and then redirected closing funds through a network of US-based money mules to the destination in Africa. The cybercriminals were brought to books by a collaboration between law enforcement officials from the US and Ghana.

# The Enterprise

- The group had two main objectives
- 1. Trick and deceive businesses into wiring funds into accounts controlled by Enterprise using email accounts tat spoofed or impersonated employees of a victim company or third-parties engaged in business with a victim company.
- 2. Conduct romance scams by using electronic messages via email, text messaging, or online dating websites to delude victims.
- During the COVID-19 pandemic, Enterprise submitted fraudulent loan applications through the Economic Injury Disaster Loan. They submitted the loan applications in the names of actual companies, but when the loans were approved, the funds were deposited into accounts controlled by the members of the group.
- Some members of the group received the proceeds of the fraud in accounts they controlled in New York, New Jersey and Virginia, who then remit the money to other members in Ghana.The group were apprehended by US authorities, in collaboration with Ghanaian authorities.

# The UMB Cyber attack

- A cybercrime syndicate made up of Nigerians and Ghanaians attempted transferring GHC326 million from the vault of Universal Merchant Bank (UMB), electronically.

- The bank detected that the amount was transferred electronically into the internal operational accounts of UMB and subsequently credited to the accounts of certain customers.
- This cybercrime is regarded as the biggest ever cyber-crime in recent times in the country.
- The bank after said after detecting security breaches alerted the Financial Forensics Unit of the CID, who dispatched personnel to all branches of the bank to arrest persons who will visit the branches to withdraw money from some identified accounts credited with the money.

- The Criminal Investigation Department (CID) arrested 12 suspected criminals.According to the police, all the suspects are believed to be part of a wider cyber-crime syndicate made up of Nigerians and Ghanaians.

# Deductions and lessons

- Cybercriminals can be people of all ages, even minors.
- New technology such as bitcoins have made payment easier for cybercriminals to demand ransom.
- Cybercriminals use social circumstances to orchestrate scams.
- The criminals could target victims in different countries.
- Cybercriminals in Ghana have a network including individuals in various countries to orchestrate the scam.
- Cybercriminals in Ghana fraud people and organizations in Ghana and abroad.
- Collaborations among law enforcers in various countries helps in the arrest of criminals, especially the criminal syndicates.
- Collaboration between victims and law enforcers also aid the investigation and arrest of cybercriminals.

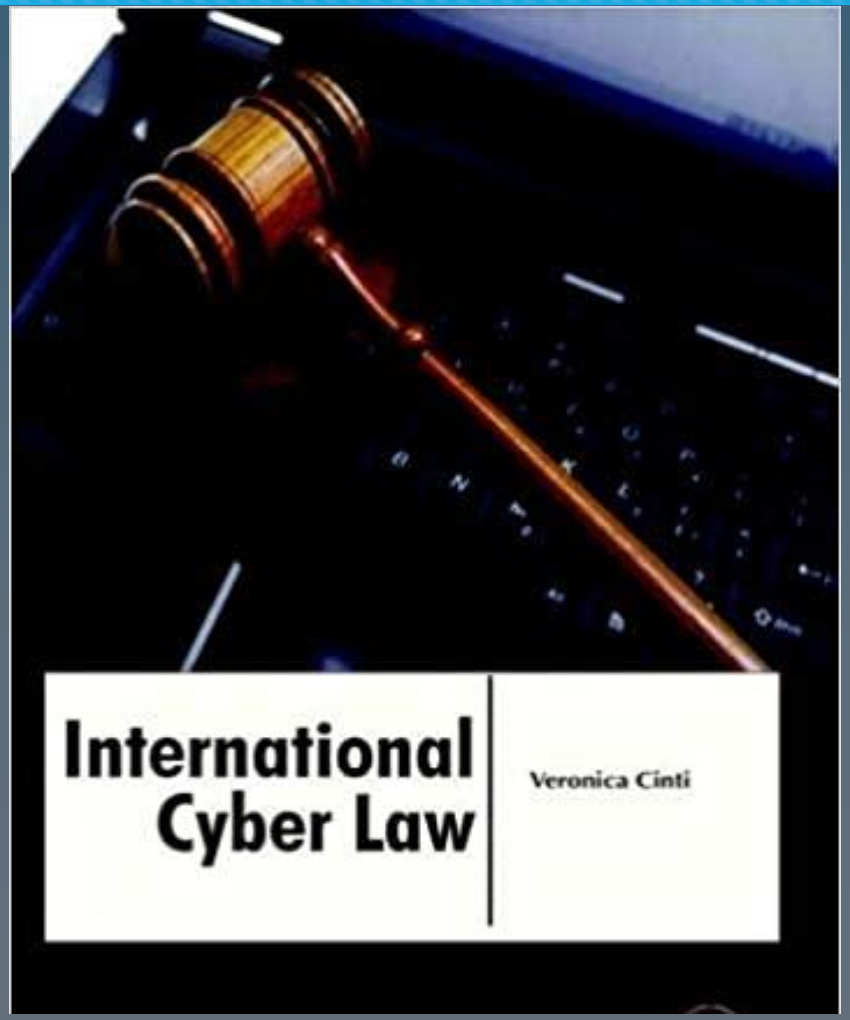
- Some crimes maybe unintentional.
- Cybercriminals hire their services.
- Rival organizations could launch or hire a cybercriminal to launch cyberattacks on competitors.

# QUE POUVONS NOUS FAIRE?

WE ARE SEEING A SIGNIFICANT SURGE IN OFFENSIVE CYBER OPS FROM BOTH STATES AND NON-STATE ACTORS.

MUCH HAS BEEN SAID ABOUT THE SITUATION.

WHAT I AM ABOUT TO DO, IS TO TALK ABOUT THE OTHER SIDE OF THE COIN - WHAT YOU CAN DO ABOUT IT



# INTERNATIONAL LAW RESTRICTIONS ON OFFENSIVE CYBER OPERATIONS

POINT 1 - THERE IS AN INTERNATIONAL LAW GOVERNING RESPONSES TO OFFENSIVE CYBER OPERATIONS COMMITTED ON OR AGAINST THE TERRITORY OF ANOTHER STATE

# THE BIG THREE PROHIBITIONS

- PROHIBITION AGAINST USE OF FORCE
- PROHIBITION OF NON-INTERVENTION, and finally or perhaps the most important one,
- NON-VIOLATION OF STATE SOVEREIGNTY

# CAPACITY: INT'L LEGAL PERSONALITY

- WHAT YOU ARE GOING TO FIND OUT IS THAT, FOR THOSE IN THE PRIVATE SECTOR THE ANSWER IS NOT MUCH. NOT MUCH WITHOUT THE COOPERATION OF THE STATE THEY ARE OPERATING IN.

- HOWEVER, FOR THOSE IN THE PUBLIC SECTOR THERE IS A LOT THAT CAN BE DONE.

# ATTRIBUTION IN INT'L LAW

- An abstract entity like the state, can only act through human actors. Through "attribution" the conduct of human actors, through commission or omission, are regarded as that of the State for purposes of fixing responsibility for an internationally wrongful act (IWA). Along with a breach of a legal obligation, attribution is one of the constitutive elements of an IWA by a State. Article 55 ASR, entitled lex specialis, provides however, that the Articles "do not apply where conditions for the existence of an IWA are governed by special rules of international law."

# ATTRIBUTION

- IF A PRIVATE ENTITY IS TO RESPOND, OR IS RESPONDING, IT NEEDS TO BE UNDERSTOOD: RULES OF JURISDICTION AND SOVEREIGNTY APPLY - THAT IS THE STATE IN WHICH THE PRIVATE ENTITY IS LOCATED OR FROM WHICH THE CYBER OPS ARE BEING MOUNTED HAS AN OBLIGATION TO ENSURE THAT ITS TERRITORY IS NOT BEING USED AS A BASE FOR THE CONDUCT OF HOSTILE OPERATIONS AGAINST ANOTHER STATE. IN THAT RESPECT, THE STATE HAS AN OBLIGATION TO END THE OPERATIONS.

- THE STATE NOT THE PRIVATE ENTITY GETS TO RESPOND BECAUSE OF SOVEREIGNTY - WHAT PRIVATE ENTITIES CAN DO IS TO COLLABORATE WITH STATE AUTHORITIES. IF THE STATE SAYS YES, THE PRIVATE ENTITY BECOMES AN AGENT OF THE STATE AND WHATEVER IT DOES THEREFROM IS ATTRIBUTABLE TO THE STATE, NOT THE PRIVATE ENTITY.

# ATTRIBUTION

- Attribution to the State is express if the acts constitutive of IWA were committed by organs, persons or the State's own agents wholly or in part, on the instructions or directions of the State, or under its effective control. (See ILC Articles on State Responsibility (the Bosnian Genocide Case))

# RESPONDING TO OFFENSIVE CYBER OPERATIONS

- RETORTION, which is a traditionally lawful response
- COUNTERMEASURES in the legal sense,
- the PLEA OF NECESSITY and finally the remedy that everyone wants to talk about all the time
- SELF DEFENCE; but which usually almost never applies

# RETORTION

- You could attempt interdicting and indicting foreign operators in the High Court of Ghana under international criminal law enforcement. But it's not that easy, the one remedy we see most often, is a remedy termed RETORTION, and we see it in response to almost every state operation against another state, where that victim state wants to respond.
- RETORTION is an act that is unfriendly, but nevertheless lawful. So for example in case of the alleged Russian hacking into the US General elections, what did President Obama do? He imposed economic sanctions and he kicked out some Russian diplomats.

# COUNTERMEASURES

- First, when you think of the term countermeasure, I want you to understand it is a legal term that has legal meaning. We are therefore not talking about countermeasures in the classic sense. I am therefore not referring to practical measures a State can take to put an end to an operation. I am talking about the legal actions or an action with legal consequences.
- COUNTERMEASURES refers to reprisals not involving the USE OF FORCE. In other words, it refers to non-violent acts which are illegal in themselves, but become legal when executed by a state in response to the commission of an earlier illegal act by another state towards the former.
- Qualification - (Condition Precedent) - Internationally Wrongful Act

# THE PLEA OF NECESSITY

- International law permits State X to hack back, if its essential interests are being affected, if its critical infrastructure are gravely and imminently affected and hacking back is the only way for the State to safeguard its essential interest against grave and imminent peril

# THE PLEA OF NECESSITY

- The plea of necessity may not be invoked unless the response is the only way for State x to safeguard an essential interest and the response does not seriously impair an essential interest of the State or the international community as a whole.
- Under the Articles on Responsibility of States for internationally wrongful acts (articles on state responsibility) by the ILC the plea is not available if State X itself contributed to the situation of necessity.

# SELF DEFENCE

- SELF-DEFENCE is found in the UN Charter under Article 51. In the cyber context, it is only available in situations of a CYBER “ARMED ATTACK”. Now UN GGE not once but twice stated that the Charter applies in cyberspace. Article 51 is part of the Charter so without doubt the international community has agreed that the LAW OF SELF-DEFENCE applies in cyberspace; but in 2017 that consent has appears to have broken down. Russia, Cuba and certain states decided they did not want the term self-defence in the report in 2017 and so it is problematic.

- The 2.4 Rule in International Law

# SELF DEFENCE

CYBER-ARMED ATTACK - A cyber armed-attack presumes significant destruction or injury. Whether cyber ops having a massive adverse effect on economic infrastructure qualifies is an unanswered question in international law, although I believe the answer is yes.

- However, SELF-DEFENCE is not available to operations by non-state actors unless those actions are attributable to the State. What you do in such cases is, you call the cops, it's a law enforcement situation.

# THANKS

Ready for your questions.