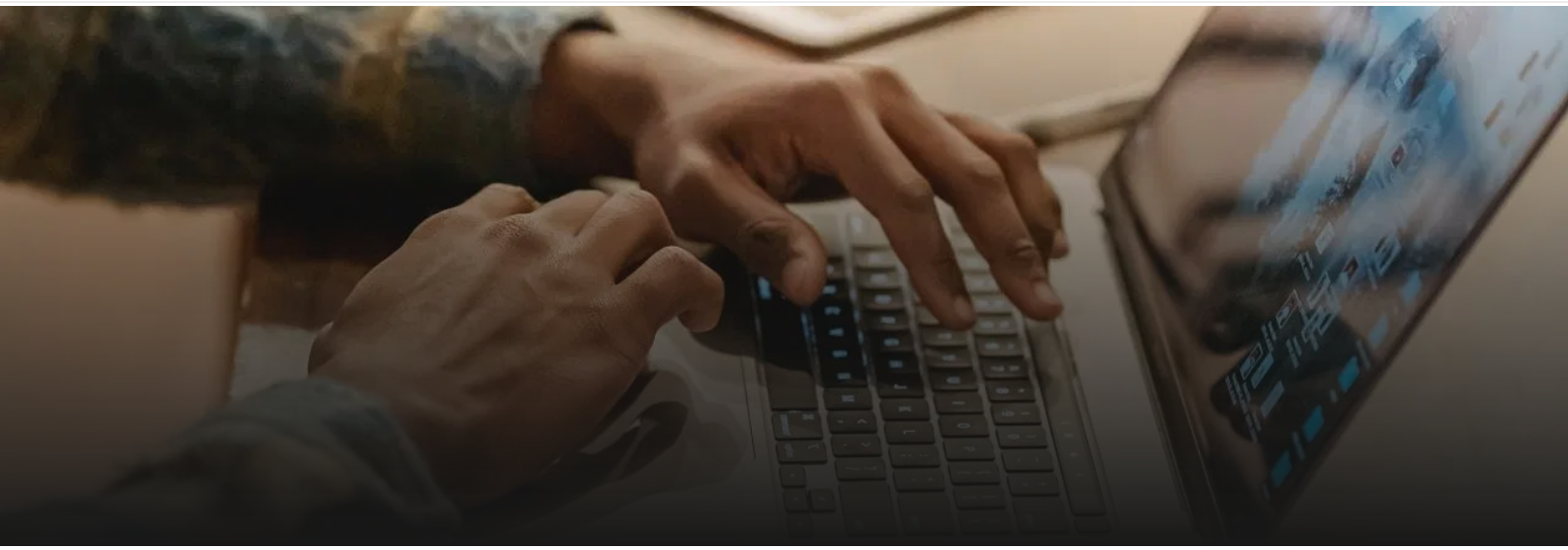

Uche Igwe

June 9th, 2021

Nigeria's growing cybercrime threat needs urgent government action

Estimated reading time: 5 minutes

Cybercrime is on the rise in Nigeria with both an increasing number of victims and perpetrators. LSE Fellow Uche Igwe discusses the economic cost to the country in the global context, and the reasons why the Nigerian government should focus on collaborative interventions.

He disguised himself as a philanthropist and businessman who flaunted his wealth with unique flamboyance and penetrating audacity. He would regularly adorn himself with fancy watches, designer clothes and showcase an expensive car collections typical of a superstar. He hung out in style with other personalities and travelled around the world in private jets and luxury yachts, displaying bundles of US dollar notes openly. He had a growing global audience of 2.5 million predominantly young social media followers. He is Ramon Olorunwa, aka Ray Hushpuppi, a man who was not exactly what he wanted the world to believe.

Hushpuppi's public drama continued until he was arrested during the COVID-19 lockdown in June 2020 on charges of conspiring to launder millions of US dollars to finance his boisterous lifestyle. According to Dubai Police, Abbas and 11 other people were arrested

during raids in which authorities seized nearly US$14 million, 13 luxury cars worth $6.8 million, 47 smart phones and computer evidence containing more than 100,000 fraud files on nearly 2 million possible victims. He has been extradited to the United States where he is currently detained and facing trial for cyber fraud, hacking and scamming.

A growing generation of lost youth

You do not need to travel far across Nigeria to see a generation of young people lost in the world of cybercrime and ostensibly inspired by the likes of Hushpuppi. You will find them in many Nigerian cities like Lagos, Benin and Owerri, and even up to Accra, Johannesburg, Dubai and Kuala Lumpur. It is from these remote locations that young opportunists try to launch phishing and ransomware attacks, including malicious spams, all over the world. Often when they try to escape criminal justice, they easily stand out with their characteristic way of dressing and brazen lifestyle.

Some of these cyber criminals did not complete their education while others are high school graduates or even students. Many address themselves as 'yahoo boys' – a known term in Nigeria for cyber criminals, suggesting that they are unashamed of their practices. Those in Accra describe their enterprise as 'pressing computer'. Osahon Ehisogie (not their real name) explained to me how many young people go the extra mile to employ the services of spiritualists, apparently to control their victims telepathically to yield to their deceitful demands.

The world of cybercrime is sophisticated and transnational, spanning across multiple jurisdictions. It has become a coordinated cartel infrastructure involving actors across the world, though how they work precisely remains a subject of investigation. Although many unsolicited phishing emails in circulation worldwide are known to originate from Nigeria, the volume of cybercrime emanating from the country is small compared to the number of cybercriminals from China, United States and Turkey. A recent report from the Federal Bureau of Investigation (FBI) listed Nigeria as the 16th country worst affected by cybercrime, and the rising number of scammers in the country is somewhat of a new phenomenon.

The reason for this increase in Nigeria is often said to be a consequence of an erosion of societal values, arising from a growing negative influence of politicians who rise to wealth suddenly through appropriating state resources for private purposes. That one does not need any special qualification to engage in politics means that someone can get rich overnight if he assumes public office. This get-rich- quick syndrome is a huge influence as young people try to make it at all costs, including through crime. But there are other

drivers, too; poverty, unemployment and inequality rates are on the rise. Cybercrime appears attractive to many partly because the probability of getting arrested is low, and many of these criminals have the physical and technical resources.

A worldwide phenomenon eating deep into the global economy

Cybercrime has become a universal spectacle, and ubiquitous internet connectivity supports cybercrime activities such as raiding bank accounts, identity theft, impersonation and stealing corporate information. Nearly two thirds of people who use online services (more than two billion individuals worldwide) have had their personal data stolen or compromised, which includes global North countries such as the UK where two thirds of the world's largest businesses suffer annual data breaches. The worldwide move to remote home working is said to have contributed to a boom in the industry.

A report by the Center for Strategic Studies revealed that cybercrime cost the global economy as much as $600 billion or 0.8% of global GDP in 2017 and will hit $1 trillion for 2020. It ranks third behind government corruption and narcotics as a global economic 'scourge', amounting to a 14% tax on growth. Online fraud and cybercrime account for half of all the crimes in the United Kingdom (5.5 million offenses annually). The United Arab Emirates is said to be the second most targeted country in the world, where the cost of cybercrime is estimated at $1.4 billion per year.

Government efforts to fight cybercrime is useful but insufficient

Like in many countries across the world, cyber-attacks increased in Nigeria during the pandemic because forced restrictions and a lockdown meant that people remained indoors. Consequent job losses led to many young people whose livelihood were under threat entering cybercrime for financial security. In response, the Central Bank of Nigeria called for increased public vigilance.

While the Nigerian Cybercrime Prevention and Provision Act 2015 has been a useful deterrent, it has been largely inadequate in preventing the vulnerability of major institutions like banks. Real-time coordination has been a challenge and made early detection and prevention difficult and insufficient. Furthermore, some unscrupulous law enforcement agents still try to take advantage of the legislation to harass young people, connive with perpetrators to procure hasty plea bargains in order to benefit from the proceeds of their crime.

Risk management and prevention

A case in point was during the recent #ENDSARS protests: many websites of several sensitive government institutions were attacked, leading to disruptions and alleged losses running into millions of naira. The Nigeria Cyber Security Outlook recently published by Deloitte revealed that phishing schemes will possibly become bigger and bolder, in addition to government and public institutions facing data leaks and sensitive information breaches. These attacks could grow increasingly daring, creative and sophisticated to exploit weaknesses in controls around payment authentication, verification and authorisation. Dealing with the criminal enterprise sustainably means foiling attacks before they happen, and urgent action is needed.

A robust and comprehensive risk management and cyber security measure is therefore urgent. While the National Cyber Security Policy adopted in 2014 outlined strategies for private sector partnership, multi-stakeholder partnership and international cooperation, recent events call for stronger synergies, regular stakeholder feedback and periodic reviews every five years, as the policy agreed. The government must be seen to be more stringent on cyber security measures with targeted enforcement, and organisations must pay more attention to cyber security and surveillance through multi-factor authentication mechanisms.

But there is also an opportunity: increased international collaboration to support information sharing and public awareness programmes on cyber security could be a trigger for global collective action. In so doing, reorientation of young people away from cybercrime must be made central to such a programme, before criminals like Ray Hushpuppi become their role models.

Photo by Andres Ayrton from Pexels.

About the author

Uche Igwe

Dr Uche Igwe is a Senior Political Economy Analyst and Visiting Fellow at the LSE Firoz Lalji Centre for Africa. He is also a Visiting Fellow at International Centre for Policing and Security at the University of South Wales. He may be reached at: ucheigwe@gmail.com.