

Not every crime is a cybercrime – The dichotomy of cyber-enabled crimes and cybercrimes

7 September 2022 5 min read

The global adoption of digital technology is rapidly increasing, which increase has caused an evolution in criminal behaviour resulting in the increased occurrence of cyberattacks on businesses and individuals respectively.[1]

The term cybercrime is used more and more often and indeed cybercrime has become the umbrella term used to describe two closely linked, but distinct ranges of criminal activity.

Most recently in South Africa and on or about 8 July 2022, two Nigerian nationals were sentenced to seven years behind bars after they cloned a law firm's email accounts and stole over R11m from its clients.[2]

But not all cybercrimes are the same! And this is very important to understand when one thinks about the newly enacted Cybercrimes Act, 19 of 2020 (Cybercrimes [Act](#)).

There is the general confusion and lack of understanding as to what exactly constitutes a cyber-enabled crime compared to a cyber-dependant crime and at the end of the day what is a cybercrime. A clear meaning as to what constitutes a cyber-enabled crime and cyber-dependant crime is vital as even small variations in the meaning could affect the measurement of and response to the crime.[3]

What are cyber-enabled crimes?

Cyber-enabled crimes are traditional crimes, which can be increased in their scale or reach by use of computers, computer networks or other forms of information communications technology (ICT).

Unlike cyber-dependent crimes, they can be committed without the use of ICT.

Fraud and theft are the most common forms of cyber-enabled crimes. There are numerous forms of cyber-enabled fraud, for example, online banking fraud, e-commerce fraud being fraudulent financial retail online sales, fraudulent sales through online auction or retail sites or through bogus websites advance fee scams such as the 4192, phishing scams are a particular kind of mass-marketing fraud: they refer specifically to the use of fraudulent emails disguised as legitimate emails that ask or 'fish' for personal for example, passwords or bank account details[4]. And then the inheritance frauds, fake charity or disaster relief frauds, fake lotteries and pyramid schemes and 'Online romance' (or social networking/dating website) frauds.

The mere fact that these crimes occur using the internet as a tool during the crime for instance an email, does not make it is cybercrime in terms of the Cybercrime Act!

Cyber-dependent crimes fall broadly into two main categories[5] –

- Illicit intrusions into computer networks, such as hacking; and
- the disruption or downgrading of computer networks and systems, such as malware and Denial of Service (DOS) or Distributed Denial of Service (DDOS) attacks and introducing viruses, worms, spyware, Trojans into networks.

Cyber-dependent crimes are committed for many different reasons by individuals, groups and even sovereign states. For example –

- highly skilled individuals or groups who can code and disseminate software to attack computer networks and systems, either to commit crime or facilitate others to do so;
- individuals or groups with high skill levels but low criminal intent, for example protest hackers;

- individuals or groups with low skill levels but the ability to use cyber tools developed by others;
- cyber-terrorists who intend to cause maximum disruption and impact;
- Other states and state-sponsored groups launching cyber-attacks with the aim of collecting information on or compromising; and
- Insiders or employees with privileged access to computers and networks.

These, amongst others, are the crimes that are provided for in terms of the Cybercrimes Act.

Turning to the two Nigerian nationals who were sentenced to seven years imprisonment, it is understood that^[6] –

- They were prosecuted under the auspices of the Commercial Crimes Court and pleaded guilty to 24 charges of theft and fraud.
- They cloned email accounts of law firms that handled property sales and registration on behalf of their clients.
- They would send their banking details to the conveyances, as though these emails were from clients. This resulted in R7.8m and R4.2m being diverted to their accounts.

Education is of critical importance given the ever-increasing rate of and proliferation of cybercrimes. In the words of Barack Obama –

“We design new defenses, and then hackers and criminals design new ways to penetrate them. Whether it’s phishing or botnets, spyware or malware, and now ransomware, these attacks are getting more and more sophisticated every day.”^[7]

Please contact us should you require cybercrime advice. Read more on the [major cyber security risks to your business here](#).

Foot Notes

[1] See K Phillips *et al* “Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies” Forensic sciences 2022, 2.

[2] See S Bhuta “Seven years behind bars for two Nigerians after R11m theft from law firm in email cloning scam”, accessed on 31 August 2022.

[3] See K Phillips *et al* “Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies” Forensic sciences 2022, 2.

[4] [Chapter 2: Cyber-enabled crimes-fraud and theft](#), accessed on 1 September 2022

[5] [Cybercrime – prosecution guidance](#), accessed on 1 September 2022

[6] *Supra* note 3 above.

[7] Pres. Barack Obama addressing the White House Summit on Cybersecurity and Consumer Protection held at Stanford University on 13 February 2015, as cited in S Kader and A Minnar “Cybercrime Investigations: Cyber-Processes for Detecting of Cybercriminal Activities, Cyber-Intelligence And Evidence Gathering” Acta Criminologica, 2019 Vol 32, No 1.



Ahmore Burger-Smidt

Head of Regulatory

[View Profile](#)