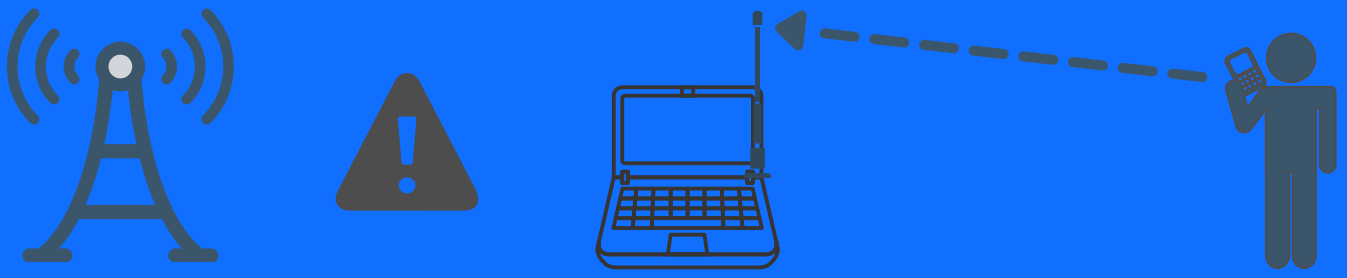
ADDENDUM: OTHER TECHNOLOGIES TO WATCH

THE IMSI CATCHER

An IMSI catcher is a portable device that can locate a person by picking up on the location of their mobile phone. IMSI stands for international mobile subscriber identity, and it is a 14 to 15 digit number that is tied to a mobile phone sim card. Each sim card has a unique IMSI number. When you register your sim card, as is required by the Regulation of Interception of Communications and Provision of Communication-related Information Act of 2002 (Rica), you must provide your name and national identification number, as well as proof of address to the telecoms operator. Your mobile service provider has this information on record. This means that you can be identified through your IMSI number.

.



The IMSI catcher takes advantage of the fact that a mobile phone must connect to the cellular network through a base station. (The base station, together with the cell phone mast and the antenna mounted on top of the mast, form a cell site. This is the most commonly visible part of the network.) The IMSI acts as a mini-base station. The surveillance targets'mobile phone does not recognise that it is not a real base station, and connects to it as if it is connecting to the actual network. Once this happens, the person operating the IMSI catcher can locate the surveillance target. More advanced IMSI catchers can listen in on conversations, read messages on the phone, and intercept data communications. IMSI catchers are colloquially known as "grabbers". Although the South African Police Service does own and utilise IMSI catchers, publicly available information suggests they are not widely used and are regarded as specialist equipment. There are no laws expressly governing the use of IMSI catchers in South Africa.

SPYWARE

Spyware is a type of computer virus, or malware, that is designed to secretly penetrate a computer or smartphone, collect the data on the device, and send it to either the government intelligence agency or criminal organisation that wants to steal the information. Companies like Israel's NSO Group (who develop and sell spyware known as Pegasus) sell only to governments. Spyware like Pegasus can be installed on a phone without requiring any interaction from the user of the phone. This is referred to as a 'zero-click' exploit. The spyware can be transmitted in a message to a phone, and downloaded onto the phone, without the user opening the message, downloading any files, or clicking on any links. It requires sophisticated forensic analysis to determine if Pegasus has been installed on a mobile phone.

Once installed, Pegasus can intercept voice calls, emails, web browsing, and messaging services, as well as turn on a phone's microphone or camera. Simply put, a government spy can remotely break into a smartphone and have the same control over the device that its user has. Encryption therefor becomes obsolete. Because Pegasus exploits vulnerabilities that the manufactures of Apple iPhone and Google Android operating systems are not aware of, there is very little a user can do to protect their phone.

Spyware sold to governments are usually meant for very targeted surveillance, aimed at political leaders of other nations, or activists, journalist and academics who may be speaking out against government. It is not a form of bulk surveillance. It is extremely difficult to regulate the use of such software because of its highly covert nature and the specialised skills required to detect the spyware on a device. Pegasus is one of several weaponised spyware software programmes available to governments.