Denel's Cutting-edge technologies leading In The 4th Industrial Revolution

25 January 2019

By Mark Minnies

The defence and national security environments have often, in the past, merely used commercial and off-the-shelf products to meet their Information and Communications Technology (ICT) needs. Not much concern or attention was paid to where the equipment and the ICT service or network was coming from.

With the fourth industrial revolution, the rapid growth of the internet and the speed at which the cyber environment is developing, we are forced to look again at WHO we are allowing in our sovereign and security spaces. The speed at which cyber technology is developing and the vulnerabilities that come with it, force us to sit up and question who is running the country's IT networks for the Presidency, Defence, Justice, Police, Emergency Services and other strategic national infrastructure. Other critical national infrastructure is all managed through a network of ICT systems including the national payment system of banks, the national electoral system, water, energy, home affairs, transport, border control and the national government's Cloud Programme.

These critical national infrastructure elements of Government are extremely exposed taking into account the capabilities and reach that cyber rogue elements have at their disposal today.

For this reason, decision makers in national security matters should increasingly ask the questions of where the hardware and software are coming from and who is the service provider? Where are the possible leaks and vulnerabilities and could we be held to ransom from our own assets and information? In other words, do we have credibility and integrity in the national systems we employ?

If this leaves Government concerned, what would be a possible solution?

This is where a trusted government technology partner comes in. A technology partner that is familiar with and trusted in the national defence and security environment. A technology partner that freely operates in, and has access to national key points. A partner with security-vetted personnel that are trusted with sensitive technology solutions. A technology partner that is familiar with systems thinking and has ample systems engineering capabilities to ensure the credibility of the IT Systems deployed.

This is the thinking and vision of the newly established Denel Sovereign Security Solutions (Denel S3) division. Denel S3 is preparing for the new digital wave in technology that is sweeping through our global society. We are developing solutions and training staff with a specific focus on software technology and software integration in particular. This implies the ability to work with various software subsystems, sensors and sub-suppliers to deliver bespoke systems that comply with the highest levels of security and integrity.
The areas and projects identified by Denel S3 include:

- CMIS environment in Defence and Defence Intelligence

- SSA IT and Cyber technology environment
- Sensitive technologies in Home Affairs
- Integrated systems in the national border environment
- Sensitive technologies and networks in the the Justice department
- Sensitive technologies and networks in the policing environment
- Strategic Partner to SITA for sensitive national security technology areas

This simply means that the state could use its own technical engineering resources to take care of its own national security challenges. This will ensure that Government has comfort in who it allows in its sovereign spaces and environments. It further means that the state has its own government-owned technology partner that takes care of the integrity of the national systems we employ. The Defence Review 2015 makes special mention of Denel as a role player in technology areas regarded as sovereign in nature.

With the support of Government, this initiative would mean that Denel is actively preparing for developments in the digital age. Denel's existing capability in the digital space is confined to the deep software capability that drives its missiles, UAV's, artillery and aerospace products. This software capability can be expanded with the training and developing of human resources in software integration in particular (we already have capabilities in electronic and mechanical) for the development of bespoke software solutions, combining various software subsystems, electronics and sensors.

Should government support the efforts of Denel S3 in the digital space for national security- related programmes, one can assume improved integrity in national systems. Other advantages include the increased development of digital skills of government human capital instead of the current over-reliance on the private sector – and in some instances of foreign origin. It could also lead to an increased demand for locally developed software sub-systems instead of the current widespread practice of supporting foreign software locally.

Denel will in future increasingly explore working with local companies with locally developed technologies who will in turn contribute to providing complete solutions in the digital environment.