Aardvark Newsletter

#7

In this Issue:

Our Sponsors

ARMSCOR
CSIR
gew technologies
IMT
peralex
SAAB
sysdel

Aardvark Roost Board of Directors

After five years of dedication to the Aardvark Roost, some of the board member's terms have expired, and they have requested not to make themselves available for re-election due to other obligations.

These members are the outgoing president, Gerrie Radloff, the treasurer, Molahlegi Molope and Brig Gen Abrie Coetzee. Their dedication and passion with which they served the local EW community will be sorely missed.

But now for the good news. We are fortunate to welcome to the Aardvark Roost Board of Directors the following members:

1. **Mirriam Molekoa from Armscor as treasurer.**

Mirriam started her engineering career at Transnet Freight Rail in 2003 as an electronic engineer where she was extensively involved on embedded software and hardware designs for railway system engineering applications. She was introduced to the defence industry and community when she joined the CSIR in 2008 as part of EW applications team in a project management role and in the latter part of 2010 she moved to Denel Land Systems. She is currently employed at Armscor as a technical manager in involved in the management of various Radar and EW technology and acquisition programs in support of the DoD product and system acquisitions.

2. Lt Col Frikkie K Schoeman as the SA Army representative.

Frikkie started his Military career in 1989 in the South African Signal Corps. He became an Officer in 1995 and filled a number of training, operational and Command posts. He was transferred to 5 Signal Regiment in 2011 where he joined the EW community as the Tactical and Mobile Unit Commander and is currently appointed as the Static Unit Commander.

3. Ryno van Staden from the CSIR.

Ryno joined the South African Air Force (SAAF) in 1998. He obtained his B. Eng (Electronic) degree at the University of Pretoria in 2002 and was utilized as electronic engineer at the SAAF 5 Air Supply Unit (ASU) Engineering Services up to middle 2003. From middle 2003 up to 2007 he was Systems Engineer responsible for airborne Infrared (IR) self-protection systems and countermeasures at the SAAF Electronic Warfare (EW) Centre.

In 2007 he left the SAAF to join the then Grintek Ewation (currently GEW Technologies) as Senior Systems Engineer with the focus on distributed strategic Communication Intelligence (COMINT) systems.

In 2012 Ryno joined the Optronics Sensor Systems (OSS) competency area of CSIR's Defence, Peace, Safety and Security (DPSS) business unit as Senior Researcher in the field of IR EW. He recently completed his B.Eng (Hons) degree at the University of Pretoria with he focus on Electronic Warfare and is a registered engineer at the Engineering Council of South Africa and a member of the South African chapter of the International Council on Systems Engineering (INCOSE).

Upcoming Events

Little Crow Conferences

As has become regular practice over the years when we don't have our biennial two day international EW conference, the Aardvark Roost plans to host 3 "Little Crow" half-day conferences again this year. The dates and venues for these conferences are:

- Little Crow #9: 22nd May at IMT, Simon's Town.
- Little Crow #10: 7th August at SAAB, Centurion.
- Little Crow #11: 17th November at the CSIR, Pretoria.

Annual General Meeting (AGM)

No dedicated AGM is planned for 2014, but instead, the Board will give an abbreviated feedback of the years achievements and activities during the last Little Crow conference on the 17th November.

International Events

51st Annual AOC International Symposium and Convention: 6 – 9 Oct 2014, Washington DC, USA.

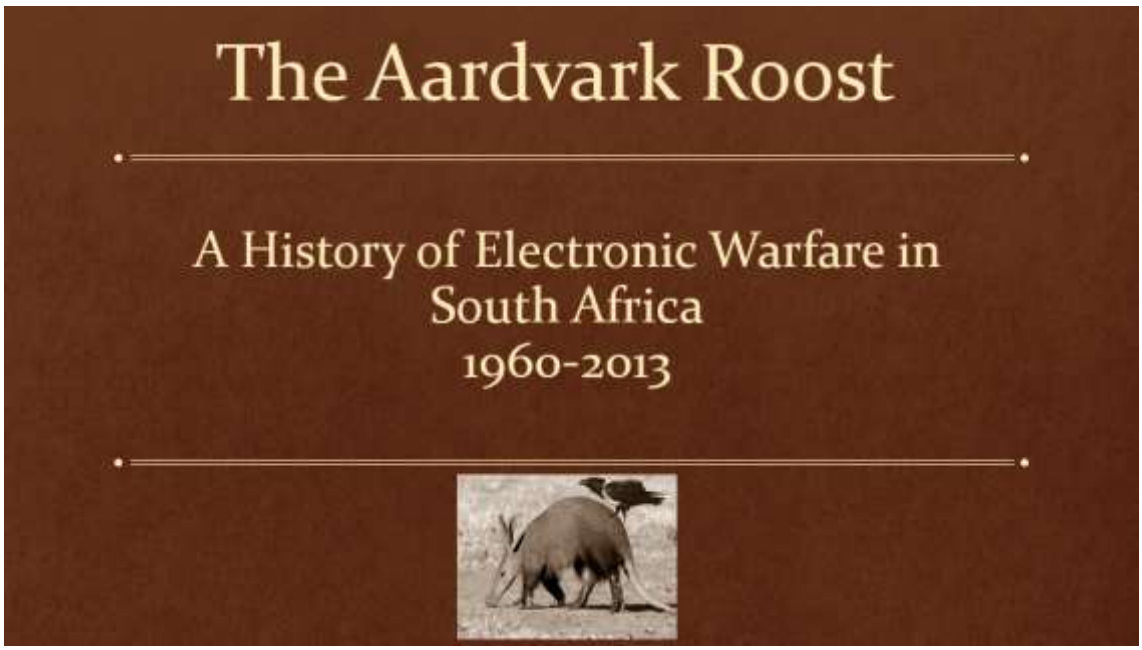
The theme will be: *Electromagnetic Spectrum Operations in Contested and Permissive Environments*

Appointments in the SANDF

The SANDF announced some new appointments and/or promotions. Some of these are listed below, as they may directly or indirectly influence the local EW, Informations Operations and Cyber environment.

CMI	SA Army	Col H.E. Gunter promoted to Brig Gen as Director JISM Post.
J Ops	SAAF	Brig Gen T. Jacobs appointed as Director Support.
	SA Army	Brig Gen T.R. Mandela appointed as Director Conventional Operations.
	SA Army	Brig Gen S.J.M. Motau appointed as Director Operations Support.
	SA Army	Brig Gen M. Jumat appointed as Director Senior Liaison Officer.
	SA Navy	R Adm (JG) P.T. Duze appointed as Director Force Prep.
	SA Army	Brig Gen B.C. Gildenhuys appointed as Director Operations.
Def Int		Brig Gen D.J. Janse van Rensburg appointed as Director Tec Int.
	SA Army	Brig Gen N.F. Maphoyi appointed as Director Intelligence Support.
	SA Army	Col M. Sizani promoted to Brig Gen as Director CI Overt Collection.
	SAAF	Col X. Tshofela promoted to Brig Gen as Director Electronic Collection.
	SA Army	Col M.J. Stiles promoted to Brig Gen as Dir Integration and Dissemination
Def Material Division	SAAF	Col L.L. Mtirara promoted to Brig Gen as Director AF Acq.
SA Air Force		Col J.C.J. Butler promoted to Brig Gen as Director Air Combat Systems.
		Brig Gen O.M. Mcetwa appointed as OC AFB Wklf.
		Brig Gen P.N. More appointed as Director Ops Supp/Int.
		Lt Col P Khoase promoted to Col as SSO EW.
SA Navy		R Adm (JG) K. Naidoo appointed as D Maritime Plan.
		Cdr J.F. Roux promoted to Capt (SAN) as OC SAS AMATOLA.
		Capt (SAN) K.L. Mabula appointed as OC SAS DRAKENSBERG.
		Cdr Msikinya promoted to Capt (SAN) as OC SAS PROTEA.
		Capt (SAN) M.A. Girsa appointed as Project Officer Project SYNE
CMIS	SA Army	Lt Col R.J. Legong promoted to Col as SSO Info Management.

Progress on the Aardvark's History of Electronic Warfare Book



Those members that have looked at the Aardvark Roost website or who attended the conference back in 4th and 5th September 2013 will be aware of the project, being coordinated by the board, to capture the history of electronic warfare in South Africa. Indeed the support given at the conference was encouraging. An appeal was made for volunteers for the various sub committees namely photography, legal, ethical and security, assistant editing, and interviewing. The response to date has been disappointing and we would still dearly like people to assist. We have started collecting some photographs but many lie in industry archives and again we appeal to industry to volunteer photos to us.

One section of the book will be a tribute to leaders of industry and most of the companies for the time period being reviewed have been contacted to provide information. Once again the initial response was excellent but to date we only have submissions from EMSS and Reutech. Thanks for your participation.

The main section of the book will of course be a collection of interesting narratives about humorous events, achievements, tragedies, and general stories of interest. A substantial database is forming and we again ask anyone who has got interesting stories to tell to contact us. We would also like to hear from you even if it is to suggest candidates we could contact. I would like to thank Denis Milton from the CSIR in helping with this as well as Allan Forest who has made suggestions to cover the naval aspects.

So in summary we are sitting at 40 pages. We would like to complete the champions of industry section by the end of March so we can concentrate on the interview sections for the next few months. Any volunteers, suggestions, articles or photos can be sent to Dave Howie at dhowie@telkomsa.net

LTE Training For the Defence Industry: A Collaboration Effort

By Molahlegi Molope

A total of 21 engineers from Armscor, CSIR, Peralex and GEW attended the Long Term Evolution (LTE) course from 3 to 7 February 2014 in Pretoria. The collaboration between these companies resulted in serious cost savings per learner. The lecturer was extremely knowledgeable and has been involved with the cell phone industry since its inception. All the learners learned a lot from the course.

LTE is the next generation of mobile communication which is IP based, focuses mainly on data and promises high data rates with low latency. The current roll outs of LTE promises downlink speeds of up to 100 Mb/s and with LTE Advanced (4G) which will be rolled out in the future promising downlink speeds of up to 300 Mb/s. With these high speeds, Voice Over IP (VOIP), video streaming etc. will happen with no buffering at all. For a small monthly subscription, you can now watch great movies over the internet as if you are watching DSTV. Downloading a two hour movie of 4.7 GB over the internet at downlink speed of 300 Mb/s will only take 2.09 minutes. LTE has 44 defined frequency bands ranging from 400 MHz to 3.6 GHz with some of them planned for future usage. The channel bandwidth is flexible with choices from 1.4 MHz, 3 MHz, 5 MHz, 10 MHz, 15 MHz and 20 MHz. The greater the bandwidth, the more data bits can be send, resulting in higher data rates. For voice, LTE falls back to legacy networks such as GSM and UMTS (3G). In future, it will use Voice over LTE technology to carry voice. The benefits for the network operators of switching to LTE is that it can share some of the UMTS (3G) infrastructure thus resulting in lower costs for them and quicker return on their investment.

The collaboration of Armscor, CSIR and industry resulted in this valuable course being offered locally at a reasonable price. Understanding LTE and other telecommunication technologies is critical when choosing which telecommunication technology to use for various requirements.

Molahlegi Molope

Acting Divisional Head: CSS - Radar and EW

ARMSCOR | 370 Nossob Street | cor Delmas Avenue & & Nossob Street | Erasmuskloof Ext 4 | Pretoria

Tel: +27 12 428 3242 | Fax: +27 12 428 3088 | Cell: +27 82 850 9224

E-mail: molahlegim@armscor.co.za web www.armscor.co.za

Automatic Identification System (AIS) and Maritime Domain Awareness (MDA)

The first in a series of technical AIS articles.

By Ernie Batty, Technical Director at IMIS Global

Brief background to AIS

SOLAS vessels [those exceeding 300 tonnes] are tracked using a cooperative tracking system known as the universal Automatic Identification System (AIS). These larger vessels are required to carry a Class A AIS transponder. A large number of work vessels, inland waterway vessels, leisure craft and fishing vessels are tracked using a lower cost version – Class B AIS transponder.

These AIS transponders installed on vessels transmit a significant amount of identification, location and navigational status information on a regular basis (every 4 seconds on average). This data is received by AIS networks that are installed in ports, along national coastlines and also on satellites that are equipped with AIS receivers. The volume and quality of information received significantly enhances any national Maritime Domain Awareness (MDA) program.

AIS technology brings precision and depth of information to the MDA environment.

South Africa, through Andre van den Berg and Capt. Keith Burchell, had a leading role in creating and establishing AIS as an international standard. This South African contribution to the development of AIS shore and ship side technology began in 1995 and continues to this day through companies such as IMIS Global Limited (IMIS).

IMIS Global and AIS

Since 2001, IMIS has designed, developed, manufactured, supported, maintained and managed a number of national shore based Maritime Information Systems (MIS) that collect, process, store and display AIS data. IMIS has also seamlessly integrated INMARSAT C and Radar data for use by various maritime authorities.

IMIS has supplied national AIS networks to Canada (>100 AIS base stations on the shore), Turkey, Croatia and Australia. The IMIS AIS network product underpinning these systems operates under the brand of *MariWeb™*.

In addition to these national AIS systems, IMIS has also supplied a *MariWeb™* AIS network to ORBCOMM, a leading Satellite AIS (S-AIS) service provider. This ORBCOMM system tracks more than 130,000 AIS targets.

Additional systems have also been sold to commercial maritime information providers in Europe and the USA.

Security, safety and AIS

In the maritime security industry, AIS is often perceived as a vulnerable data communications technology that is open to abuse and misuse. However, IMIS Global, through *MariWeb™*, has introduced features that not only protect AIS networks and the information contained in those networks, but also assists in identifying sources of AIS data that are illegitimate and require further attention. These include vessels attempting to be part of the legitimate vessel fleet, as well as data sources that are attempting to 'spoof' or create fake targets with malicious intent.

For increased security of communication, AIS allows for the transmission of encrypted data between vessels, and between vessels and the shore side AIS network.

Where authorities require all vessels to be mandatorily fitted with AIS (Class A for commercial vessels and vessels carrying paying passengers, and Class B for all other vessels), safety, security, and indeed maritime economics and the maritime environment are improved. This is due to the ability of AIS to identify, locate and, where required, assist all vessels fitted with AIS. These are the significant benefits produced by the precision and depth of information that AIS networks provide.

Further, by linking AIS and Radar data, it is possible to identify vessels with and without AIS transponders, allowing authorities to focus on vessels that require further attention.

AIS technology adds significantly to the Search And Rescue (SAR) capability of any country by accurately identifying each vessel's identification and current location on a continuous basis and in case of an incident, allowing vessels in the local area to provide the required assistance.

An AIS transponder broadcasts its data to all vessels in the area thus increasing the chances of saving lives in critical or dangerous situations.

The accurate identification and location process provided by the AIS technology also extends to any persons who may have fallen overboard and are equipped with an AIS Man Over Board (MOB) equipped life jacket.

VHF Data Exchange System – the future of AIS

Due to the significant success of AIS and the need to transfer more data between vessels and between vessels and the shore, it is now proposed to expand this technology by adding additional channels (up to 6 AIS type channels) and includes higher speed (+/- 300Kb/s) data links in the VHF maritime band. This development is known as the VHF Data Exchange System (VDES).

Currently Channels AIS1 and AIS2 are used for most AIS traffic, Channels AIS3 and AIS4 are used for satellite AIS reporting. Channels AIS5 and AIS6 are being proposed for Application Specific Messages (ASM) that are primarily used to transfer information between ship and shore, such as number of persons on board.

The higher bandwidth channels will support the IMO e-Navigation goals.

Conclusion

AIS brings significant benefits to the MDA, provided that the data gathered from vessels is properly processed and presented to operators, but it is not the answer to all Environmental, Safety, Search And Rescue and/or maritime security requirements.

Should you wish to know more about AIS technology and the proposed future VDES technology, please do not hesitate to contact IMIS Global (www.imisglobal.com).

This is the first in a brief series of articles written by IMIS in connection with AIS technology and VDES, the intended successor technology to AIS. More complex matters will be addressed as each new article appears.

Industry News

Saab South Africa receives follow on orders for Self-protection System

Saab Grintek Defence (SGD) has received two orders from Hindustan Aeronautic Limited (HAL), India for serial production of an integrated electronic warfare self-protection system.

The system, which will be installed on the Indian Army's and Air Force's Advanced Light Helicopter Dhruv, will be developed and produced at Saab South Africa's headquarters in Centurion (Saab Grintek Defence) and has a total value of approximately R335 million ($ 33 million).

Saab's Integrated Defensive Aids Suite (IDAS), protects crew and aircraft and enhances the survivability in sophisticated, diverse and dense threat environments. The system provides a timely warning against different types of threats including radar, laser and missile approach warning; and automatically deploys the appropriate countermeasures.

"Saab has an unbeaten capability in the field of electronic warfare and self-protection. The IDAS system is one of our flagship products sold to customers around the world", says Micael Johansson, Senior Vice President and Head of Saab's business area Electronic Defence Systems.

Commenting on the development of the integrated system at Saab's South African base, CEO Magnus Lewis-Olsson said: "Saab in South Africa fulfils an important mandate on the African continent and beyond by delivering an impressive range of South African electronic warfare technology. Up to 90% of these systems are being designed and produced in SAAB Grintek Defence facilities in South Africa – and we are proud to deliver on this important contract."

These orders follow initial serial production orders received in 2008 and further established Saab as a local partner to the Indian Industry and provider of high tech products and systems to the Indian Armed Forces.

"With these orders we continue to build on our very successful partnership with HAL. The fact that HAL and the armed forces have continued to show faith in the IDAS system is a testimony of the effectiveness and reliability of the solution", says Lars-Olof Lindgren, Head of Market Area Saab India.

Deliveries are scheduled to commence in 2014. Development and production of the IDAS system will take place at Saab in Centurion.

Saab Grintek Defence will also undertake transfer of technology to HAL to co-produce and indigenize the self-protection system in India.

SAAB: What happens during a piracy attack?

Gareth Morris from Saab Grintek Defence (SGD) looks at local technology geared to counteract attacks in a marine environment.

According to the IMB Piracy Reporting Centre the number of piracy attacks worldwide for this year alone stands at 176 reported incidents, including 10 hijackings. The centre indicates the number of crew/vessels currently held by Somali pirates as 57 hostages.

Although the IMB indicated that piracy attacks dropped to a five year low in 2012, the number of piracy-related attacks remains high and on certain routes seafarers are still considerably at risk. In Somalia, and elsewhere, vessels most commonly attacked are container ships, bulk carriers and tankers loaded with oil, chemicals and other products. Fishing vessels and other smaller boats are also at risk.

The hard fact is that piracy against merchant vessels poses a significant threat to world shipping, and with more than 90 percent of global trade transported by sea, it is cardinal that this vulnerable supply chain is as secure and efficient as possible - but what actually happens during such an attack?

According to the World Shipping Council, in many instances Somali pirates use hijacked merchant ships as mother ships to carry out attacks in the north Arabian Sea and near the coastline of India. It explains, “pirates make use of multiple, high-speed skiffs (small attack boats) to approach and fire on the bridges of What happens during a piracy attack?

vessels with automatic weapons and rocket propelled grenades, in an attempt to slow or stop the vessels so the pirates can get on board.”

Once a vessel has been hijacked, the pirates typically request a large ransom – often in the millions of dollars as payment for the safe return of the crew, vessel and cargo.” Pirates are often supported by terrorist organisations and thus more frequently have access to more advanced weaponry, including laser guided munitions.

These pirates are often difficult to prosecute in international courts as, when confronted with a modern naval force, pirates will throw their weapons overboard to eliminate the evidence.

Gareth Morris of Saab Grintek Defence, which produces, amongst others electronic warfare technology and systems geared towards asymmetric operations like anti-piracy,

indicates that there is good news in the form of the advances made in the field of navy-protection technology. “Currently Saab has the NLWS (Naval Laser Warning System) and the SME-50 system which are not only geared for asymmetric operations like anti-piracy, but also drug smuggling, maritime terrorism and trafficking,” he elaborates. This technology is finding global application in promoting maritime

defence and security, with indigenous South African products being sold to the world market.

Morris reveals that SGD has developed numerous technology and radar electronic warfare solutions for surface ships and submarines and that this technology has been expanded to international markets like Germany and South Korea. The German Navy, for example, makes use of the SGD SME- 100 Radar ESM System as well as the SGD Naval Laser Warning System aboard its Mine Counter Measure Vessels (MCMV) which are used in United Nations Interim Force in the Lebanon (UNIFIL) operations.

“Although the chances of a laser guided missile sinking a large naval ship are slim, the damage it causes will most probably affect a mission kill. The damage to smaller vessels and commercial shipping may however be extensive. With this in mind, and the known proliferation of these weapons across the globe, ignoring this threat is done at peril. Laser guided munitions are low cost, relatively easily obtained and manufactured and operated by most countries across the world,” Morris explains.

Various types of laser threats may be encountered. These include:

Dazzlers: These lasers are specifically designed to cause permanent blindness to un-enhanced vision. Although prohibited in terms of the Hague Convention Protocol IV to the 1980 Convention they are still being used but Saab’s system does detect them as well as detecting the other systems below.

Range Finders: Range finders are the most common type of lasers encountered in the maritime environment. They range from commercial use to weapon applications and are available from a wide variety of suppliers. They are generally used for ranging or as part of the calculation of a fire solution.

Designators: Designator lasers are used to illuminate or paint a target and the missile then homes in on the reflected laser energy. The missile and the laser source do not necessarily have to be co-located.

Beam Riders: Beam rider operation requires the missile and the laser source to be co-located. In the case of the beam rider, the laser source illuminates a detector channel situated in the back of the missile. The laser source guides the missile onto the target by sending steering guidance information to the detector.

Most of the SGD ESM and NLWS systems are provided to the navies through shipyards and other Large Scale System Integrators in Germany, the Middle East and South Korea. These

systems are easily integrated with other ship systems which add to the overall safety and effectiveness of the vessel. Typical subsystem integrations include the Combat Management Suite and Counter-Measure systems.

Morris concludes: "Ships on the open seas have become extremely vulnerable targets, but it is important to stress that solutions exist to combat this vulnerability and to enhance security.”

CSIR and SAPS in partnership to expand national safety and security capacity and capabilities

The Council for Scientific and Industrial Research (CSIR) and the South African Police Services (SAPS) signed a Memorandum of Agreement that creates the institutional framework for the SAPS to access scientific, engineering and technology support for both the operational and strategic components of their duty towards national safety and security.

The Agreement is a formal step towards the longer-term objective to establish a Safety and Security Evaluation and Research Institute that will perform independent, ongoing scientific and operational research and evaluation tasks and provide scientific decision support services to the SAPS as and when required.

The Agreement outlines a portfolio of research and technology support programmes with deliverables over a three-year period.

Science to support 'smart policing'

Addressing members of the media at the signing ceremony at the CSIR International Convention Centre in Pretoria, National Police Commissioner, General Riah Phiyega, said the partnership will offer the SAPS a wealth of multidisciplinary science and research. "It will support smart planning, it will offer us smart use and management of technology and will ultimately result in 'smart policing'," she said.

"The CSIR is already working together with various government departments - including the South African National Defence Force (SANDF), the Department of Home Affairs, and Department of Health, and we have seen the fruits of that cooperation. We as SAPS are also seeking to collaborate in order to improve our efficiency and effectiveness. So, in a way this is a long overdue marriage." Phiyega said.

She referred to a few areas of improvement they would be calling upon the CSIR for support – such as tender management support, enhancement of developing programme management capabilities, technology forecasting and planning, analysis and modelling, and accreditation of forensic science activities.

"Having seen what CSIR was able to achieve for our sister departments we are not lost. We thank you for allowing us the opportunity to partner in this journey of continuing to approve SAPS and the offerings it gives to the citizens of this country," Phiyega said.

Commenting on the agreement, Dr Sibusiso Sibisi, CSIR Chief Executive Officer, emphasised the unique role of the CSIR as an impartial and independent advisor on technology: "It is imperative to understand the type of organisation that we are," he said. "We are not a player in the technology domain *per se* in the sense of being a vendor of technology products. We are positioned to act as smart advisor to assist the SAPS to be a smart buyer and user of technologies in a manner appropriate to their needs."

He continued: "The CSIR is a public institution whose mandate it is to conduct science, research, technology and innovation in order to advance the wellbeing of the people of our country. Promoting a safer South Africa is absolutely in keeping with our mandate. It is a mandate we take very seriously," he said.

About the programmes

The first programme will address **Command, Control and Shared Situational Awareness** solutions including technologies such as sensors, data fusion, intelligence and information gathering, display and dissemination, plus associated information technology infrastructure, as well as operational command and control systems and infrastructure in the form of so-called 'war rooms'. Such facilities have already been piloted and tested at the CSIR for use in large-scale national surveillance and safety operations, such as during the Soccer World Cup in 2010.

In the ICT domain, the CSIR will be focusing on optimising systems within the SAPS to improve efficiency and cost effectiveness. The programme will be conducted in alignment with the CSIR's relationship with the State Information Technology Agency (SITA), which has a distinct statutory mandate regarding ICT services for government. The CSIR's

responsibilities will lie in research, development and include next generation network systems architecting, analysis, simulation and evaluation, wireless solutions, cyber security and digital forensics.

Integration and interoperability are key means of optimising existing infrastructure and resources in defence and security. This entails finding ways for the smarter use of existing equipment and systems and avoiding new investments, the pitfalls of vendor lock-in and risks of costly, yet soon obsolete systems. This not only leads to better use of existing infrastructure but also improved connectivity within the SAPS operations and beyond.

One such area is border safeguarding, which is an issue of importance for the SAPS – but also the SANDF, the Department of Home Affairs, and National Parks on the issues of poaching and smuggling, and many others. This is an area where technology has been tested to synchronise activities between parties by establishing systems, standards and procedures for interoperability.

Dr Sibisi explained the importance of such an integrated, interoperable capability: "Whatever technology is deployed at a particular time at a particular location ought to operate in a seamless manner with others and with technologies added over time and elsewhere. This is absolutely essential if the Police Service intends to be agile and respond in an agile manner - be able to receive, process and understand the kind of input data they receive, communicate with other colleagues and forces, across services," he said; "To do that, technology must genuinely be an enabler and not a hindrance. This is our understanding of our task in this partnership: We are seeking to develop technologies that will enable SAPS to be quicker, better and tougher," he said.

Operational Quick Reaction Tasks (QRTs) are critical in agile law enforcement. This includes the ability to rapidly design, engineer and create a custom solution to an urgent operational need. Examples can include urgent deployment of overhead surveillance in areas of uprising, droppable field mission control containers, and terrain-specific vehicle adaptation. Through the Agreement, the SAPS will have access to knowledgeable, technically and operationally skilled personnel to respond to immediate needs at short notice and to provide solutions to immediate problems. The CSIR has performed this duty for the SANDF for many years. Additionally, and with a longer term view, the CSIR will perform operational assessments of current doctrine, tactics, procedures, optimising the use of personnel, systems and equipment.

The programme to drive **science and technology capability development** is set to bring skills and capabilities to the SAPS to support systems and product evaluation, acquisition, product deployment or customisation, plus to establish new technical capabilities that are currently underutilised. This is part of a global trend for police and defence forces to train staff not only in law enforcement skills, but to provide varying levels of technology competence development as well due to the role technology plays in combatting crime and understanding greater levels of sophistication in technologies used to perpetrate crime.

"Our intention is to help the Police Service be tough on crime, and tough on the causes of crime," Sibisi explained.

In the area of **Strategic and Operational Decision Support,** activities will focus on the establishment of a scientific decision support base for the SAPS for both operational and strategic needs. This will include tender support, programme and project management support (quality assurance and configuration management), strategic technology forecasting, analysis and modelling (e.g. crime statistics) and facility planning.

The ultimate aim is the establishment of a strategically independent Safety and Security Evaluation and Research Institute that will serve as the SAPS 'in house' science and research capability for ongoing evaluation, procurement support and strategic technology capability management.

Enquiries CSIR:
Tendani Tsedu
CSIR Media Manager
Tel: 012 841 3417
Cell: 082 945 1980
e-mail: mtsedu@csir.co.za

Enquiries SAPS:
Lieutenant General Solomon Makgale
Head: Corporate Communication
Cell: 082 788 3718

For any inputs/comments on this newsletter, please contact Christo Cloete at ccloete@csir.co.za or 012-841 4485.