UNIVERSITEIT
iYUNIVESITHI
STELLENBOSCH
UNIVERSITY
100
1918 · 2018

saam vorentoe · masiye phambili · forward together

RESEARCH BRIEF 16/2020

Security Institute for Governance and Leadership in Africa

SIGLA @ Stellenbosch

Author: Graham Walker (Saab Africa) **Series Editor**: Prof F. Vreÿ (SIGLA)

Embracing technology in the response to insurgency in northern Mozambique

Background

With the emergence of radical militant insurgency in Cabo Delgado in Mozambique, the South African National Defence Force (SANDF) in their military response would be well advised to adopt a broad spectrum of technological solutions available. It is also worth remembering that merely possessing technologically advanced weapons and military equipment does not ensure success. Instead, it is the art of war, or the careful, smart and measured application of available modern technologies that will ***support*** the military response and help ensure success.

Discussion

As Blaine asserted in his SIGLA Brief 13/2020 regarding "counter-insurgency assistance from the sea", the South African Navy (SAN) as part of the SANDF response may be well suited to provide their capabilities in future military operations to help curb insecurity in northern Mozambique. This maritime approach provides benefits and additional options to the SANDF if they are to embrace the range of modern technologies available. Five generic phases offering room for use of available technological systems are at play: planning, preparing, mobilising, execution and termination.

Planning

During planning, intelligence about the opponent, their intentions, their constituents, their methods, equipment and location is the single most important factor. Utilising technology to obtain information and to process this into useful intelligence is key. Technologies such as communication intercept systems may be used to monitor enemy activities. Introducing Artificial Intelligence and Machine Learning to analyse the intelligence and identify patterns or connections will prove useful to develop possible courses of action. Information sharing between regional and international counterparts is another critical component of the intelligence situation that requires a technological solution to facilitate the secure sharing of critical information.

The use of satellites for reconnaissance and surveillance purposes, combining optical imaging and synthetic aperture radar sensors to build an accurate picture of the environment and the opposition is another example of the use of technology in this first phase. The application of modern technologies including geospatial analysis of satellite imagery to detect changes in the environment and landscape and to provide clues to the developing situation within the operational theatre could prove invaluable.

Preparation

Once SANDF contingents commence mission training to confront an unfamiliar opponent, technology integration can improve training methods and instil a degree of realism for the training scenarios. Battlefield simulation and computer algorithms can be utilised to evaluate the planned courses of actions of own and opponent forces and will be useful in assessing the best approach to counter the threat. The use of simulation technologies and virtualisation capabilities do not only enhance the quality and realism of the training, but also reduces costs.

During preparation, and more importantly when facing counter-insurgency operations, the psychological aspect requires attention. In the modern era, a well-crafted social media campaign embracing multiple media platforms is required to shape the battlefield, bolster own forces' morale and garner public support for the military action. In using these technologies in the early stages of military operations, the aim is to create conditions that are favourable for own operations before the first physical contact.

Mobilising

The principle of denying your opponent freedom of manoeuvre, in both the physical and electronic domains helps own forces to maintain the advantage and momentum as they advance to the operational area. Within the scope of denying your opponent the freedom of manoeuvre, the dominance of the electromagnetic spectrum together with information superiority fosters favourable conditions within which to conduct future military operations. In the maritime sphere, the nature of asymmetric threats and counter-insurgency may employ swarm tactics against naval vessels; naval vessels that can be regarded as the Centre of Gravity for counter-insurgency operations from the sea and serve as mission essential or high-value units. It is for this reason that the range of technologies such as Automatic Identification Systems (AIS), Long Range Identification and Tracking (LRIT) coupled with the airborne technologies for Identification Friend or Foe (IFF) and Automatic Dependent Surveillance-Broadcast (ADS-B) should be fused to provide a comprehensive maritime domain awareness (MDA) picture. Having a credible and accurate MDA picture will enhance own forces' situational awareness with respect to neutral and friendly shipping and aircraft movements and allow them to focus efforts on the detection, localisation and identification of opposing forces.

Denying an opposing force freedom to manoeuvre in the electronic domain could also see own forces adopting GPS independent combat systems whilst conducting GPS jamming and spoofing activities targeted at opposing forces' networks and equipment. The opposing forces in an insurgent type conflict may have a higher dependence on commercial off the shelf systems that are susceptible to GPS jamming and spoofing although the use of available military-grade hardware is not impossible. By denying GPS syncing and time-stamp information to hardware and software systems that depend on GPS for their correct functioning, GPS jamming and spoofing capabilities offer useful counter-measures to own forces.

Execution

Recently, the greatest leap in military technologies stems from the domain of unmanned systems. For counter-insurgency operations in northern Mozambique, the adoption of Unmanned Aerial Vehicles (UAV) and Unmanned Surface Vehicles (USV) lowers the risk to human life when in contact with the opposing forces. Fixed-wing UAVs with mid-altitude and long-endurance capabilities can provide strategic and operational surveillance tasks whereas ship-borne rotary-wing UAVs can enhance situational awareness and provide tactical surveillance and monitoring requirements with a home base that is too remote and distant for reprisal attacks. UAVs can also provide an overt or covert shadowing capability for persistent observation of opposing forces. USVs in turn can be used as force protection elements for naval vessels when they may be operating close to the coast or alongside in harbour for replenishment, providing early warning of impending attacks and reducing the man-in-the-loop footprint for force protection activities.

Opposing insurgent-styled forces will most likely rely on asymmetric tactics, including swarm tactics utilising several smaller vessels against naval vessels together with attacks that derive their advantage through the element of surprise. To counter surprise attacks, the use of Electronic Warfare capabilities including communications intercept and analysis systems will be vital in supporting situational awareness of forces. In the event that opposing forces are in a position to launch an attack, warning time may be minimal and as such, early warning (such as UV flash detection) and self-protection systems that have the ability to automatically deploy active or passive countermeasures could be a critical technology to save lives.

Smart munitions and/or precision-guided munitions incorporate the latest technologies to assist military commanders to employ their firepower in an effective, efficient and responsible manner. The use of these munitions reduce collateral damage by engaging only opposing forces with little disruption to civilian lives and infrastructure. The latter has become a critical matter during counter-insurgency operations where collateral damage (human as well as material) often leads to severe discreditation of security forces.

Termination

The importance of the termination phase is often neglected. Within this last phase of a military operation an after-action review and debrief, documenting lessons learnt, archiving decisions made, operational recordings and other resources utilised must be registered. Secure information technology solutions that capture, store, reference and process this information post-operation are crucial in building and enhancing military capabilities and even more so when regional military cooperation is at play. This information must also be available for training formations in the validation of curricula and training methods as well as being available to staff officers in the development of future military doctrine and strategy – nationally and regionally.

Conclusion

The SANDF has not previously encountered IS-affiliated forces or been part of a multinational operation against these radical insurgent forces in their history. As such, they need to prepare themselves as best they can to ensure success. Seizing the advantage means introducing modern technological solutions across a broad range of capabilities and integrating them into their doctrine and operating philosophy for countering insurgent activity. For military forces, adopting and incorporating new technologies is standard routine, and for the SANDF facing this next chapter, it is a principle worth embracing. Military operations, no matter where they fall on the spectrum of conflict, require a partnership with available civil, security and cutting edge military technology solutions that will serve the SANDF well when engaging dangerous counter-insurgency actors.

Graham Walker was a former Captain (SAN) in the South African Navy and is now a Naval and Maritime Marketing and Business Development Executive for Saab's Sub-Saharan Africa Country Unit. This piece has been written in his personal capacity as he maintains a keen interest in maritime security affairs in the Sub-Saharan Africa region. E-mail: graham.walker@za.saabgroup.com