Understanding the shortcomings of PACE plans in battlefield communications

Battlefield communications are fraught with complex challenges like security, reliability, and availability. The PACE (Primary, Alternate, Contingency, Emergency) methodology, employed widely within international defence groups, provides a means of assuring communications.

Tim Williams, Business Development Manager, QinetiQ

The implementation of Command and Control (C2) communications is a complex process for any organisation and requires in depth planning. This is further exacerbated if the deployment of forces is in a region where the quality of network infrastructure is low. This challenge is one that Western military organisations are subject to regularly, given their deployments in under-developed countries such as Mali where British troops have recently been deployed to.

The ability to communicate on the battlefield is essential for coordination, reporting and C2 across the full spectrum of military operations and incorporates all functionalities from the fighting troops through to the logistics force that supplies them.

Considerations for assured tactical communications

When using mobile phones in our day to day lives, it's easy to ignore the eye-watering level of planning and implementation of the infrastructure required to make them work. In a combat scenario, the planning and implementation goes even further given forces are working within a constantly changing environment, where the infrastructure has to be built using platforms that may have to move daily (or hourly), where risk to life is high and freedom of movement is dictated by where in the battlefield you are situated and the level of dominance you have in that area. Planning considerations for tactical communications include:

- Frequency selection;
- Path profile analysis;
- Range;
- Ground layout;
- Generation and implementation of encryption;
- Terminal identification allocation;
- Location and strength of enemy;
- Potential for denial of service from electronic warfare (jamming); and
- Targeting of key nodes due to Radio Frequency detection.

Aside from these, it is important to take into account the effects of weather, terrain, and changes to the ionosphere. Many

If a deployed user does not have the ability to communicate, it can result in them returning to base and failing to complete the mission. Photo courtesy of QinetiQ

factors are outside an organisation's control and therefore drive the need for versatility and resilience to a plan.

Why the best planned communications still cause mission failures

The above merely considers the delivery side. C2 is also required for the coordination and support of the very personnel and platforms providing the infrastructure for the communications network.

How do they achieve the intricate level of engineering needed to set up the communications network in the first place? Generally, the answer is through verbally delivered orders prior to deployment which are a thorough set of instructions that try to cover every eventuality. However, the situation can change rapidly, and the relevance of those orders can dwindle. If a deployed user does not have the ability to communicate, it can result in them returning to base and failing to complete the mission.

How the PACE methodology Helps

The biggest issue is that communications routinely fail at the most critical point. To overcome this, a methodology called PACE (Primary, Alternate, Contingency, Emergency) employed widely within international defence to provide resilience to a communication plan, is adopted. This provides a means of assuring communications and ensuring all key nodes and personnel have some means of transmitting and receiving messages.

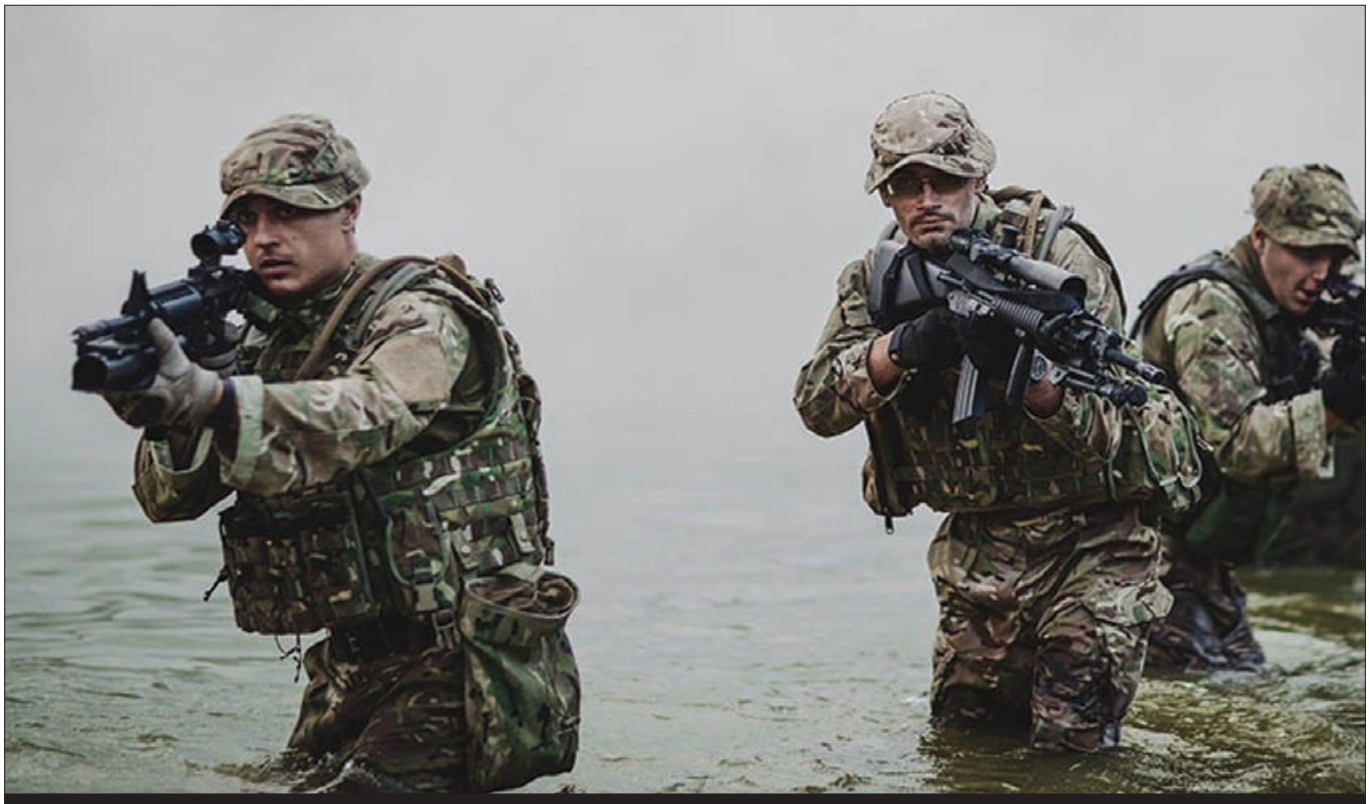
An example of the PACE process being implemented is as follows:

Primary: The primary means are usually complex, robust, digitised military communications systems that are routinely expensive, heavy in weight, large in size (vehicle borne - less some manpack solutions) and are delivered as part of a defence organisations' equipment programme. The primary system usually operates within the VHF/UHF frequency band and provides voice, data and situational awareness data services and is protected with high grade encryption. When fully functional, this system provides operations staff with the tools they need to plan and prosecute the military tasks bestowed upon them. These primary systems tend to be complex and require a high degree of training for system engineers and operators to achieve the level of competency required. Additionally, the management required to deploy systems in the simplest scenario cannot be underestimated and can take months in advance of a deployment.

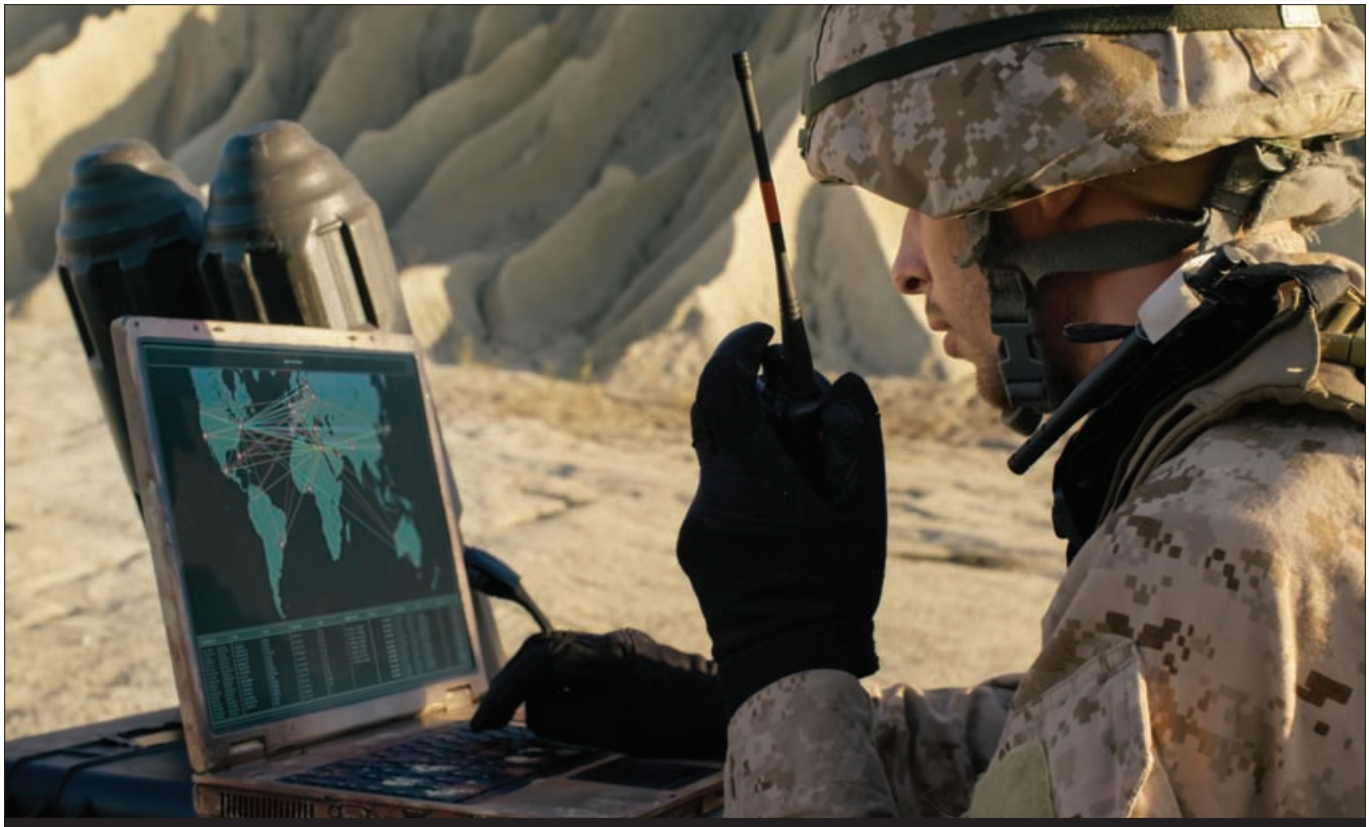
One of the biggest constraints with VHF/UHF radio systems used in a line-of-sight role is the range; distances of between 20-40 miles are achievable in normal undulating terrain, however, many operations, the ground to cover can range from 100s to 1000s of miles. Increasing the range of the links requires rebroadcast stations to be implemented, but this adds further complexity to a communications plan. Other primary systems include UHF Tactical Satellite systems, but this is dependent on limited satellite channel availability and tropospheric scatter capabilities.

Alternate: When communications fail, an operator then needs to understand whether it is a local equipment fault, issues with frequencies or weather, to mention a few. It could also be due to problems being experienced at the distant end. Engineering is required and in many cases, it requires for communications between the nodes. This requires another system, an alternate system.

In this scenario, the alternate system is a High Frequency (HF) radio. This is likely to be based on a complex and High-Grade encrypted system, which is part of a wider Combat Net Radio programme. Again, these types of radios usually require highly competent operators in order to deliver effective communications. With most HF systems it is relatively simple to establish a link over 30-40 miles by using whip type antennas or simple vertical wires. Many systems today have the ability to electronically lengthen antennas when a frequency is changed in order to minimise the effort required, whilst maximising the probability of success. This is further supported by automatic link establishment where the network chooses the best frequency to operate from. The shift from VHF/UHF to a HF



PACE is not about providing four levels of failproof communications, it is about assuring communications and keeping personnel safe in what can be highly hostile environments. Photo courtesy of QinetiQ



The ability to communicate on the battlefield is essential for coordination, reporting and C2 across the full spectrum of military operations. Photo courtesy of QinetiQ

solution will reduce the bandwidth and in turn reduce the level of data services that can be supported, which can include reduction or total loss of situational awareness position feeds.

The impact of weather, time of day, seasonal changes and atmospheric interference can be the difference between good and no communications. Whilst you can increase antenna lengths to counter the lower operational frequency which occurs at night, this will reduce mobility.

Establishing a link between 20-50 miles is relatively straight forward but achieving success between 70-200 miles is a totally different challenge and may require the use of Near Vertical Incidence (NVIS) Skywave which can test even the very best operators. The bottom line is that when you switch to HF you have to continuously work for communications continuity and with the environment changing on an hourly basis, this can be an onerous process.

When switching to an alternative system as part of PACE, the user will experience some loss in capability, whether that is quality of voice and/or reduction in bandwidth. The most important point is that HF links require engineering, and, in many cases, this requires the operator to communicate with a distant end.

Contingency: In the event the alternative system is not successful, users will then look to their contingency solution.

In a world of budget constraints and prioritisation it is difficult for organisations to invest in effective contingency communications systems. If you ask a large proportion of military communicators or operational staff what the plan is for the alternate system, they will most likely respond that it is a mobile phone. In fact, the mobile phone has probably been etched throughout the plan being used to engineer the primary and the alternative links and conduct other administrative tasks. And it's easy to understand why; mobile phones are both easy and effective. During military exercises, there are usually time constraints as many tasks need to be sequenced to test and train personnel. Additionally, there are pressures to ensure the exercise is a success. This drives a culture to use mobile phones to coordinate events. In many cases it could be perceived as being the primary means of communications. There is a military saying: 'Train as you Fight:' Adopting a culture of using mobile phones can have a very negative effect.

If we put the user in a war-torn country where infrastructure has been destroyed or in the jungle, desert, remote mountainous region or at sea, there is unlikely to be mobile coverage. This changes the playing field. It is also important to highlight that the level of security, stressed as one of the most important attributes of the primary/alternate system, has suddenly diminished from High Grade encryption to a non-secure system. When both the primary and alternative links have failed and your trusty mobile does not work, the options are either to return to base or reach for the emergency system.

Emergency: As with contingency solutions, little investment is given to emergency systems. Some of the luckier users may get a non-secure satellite phone or even a distress beacon (but we are not at the stage where a user needs to send an alert). The point here is there is a cliff drop in capability if both primary and alternative systems fail.

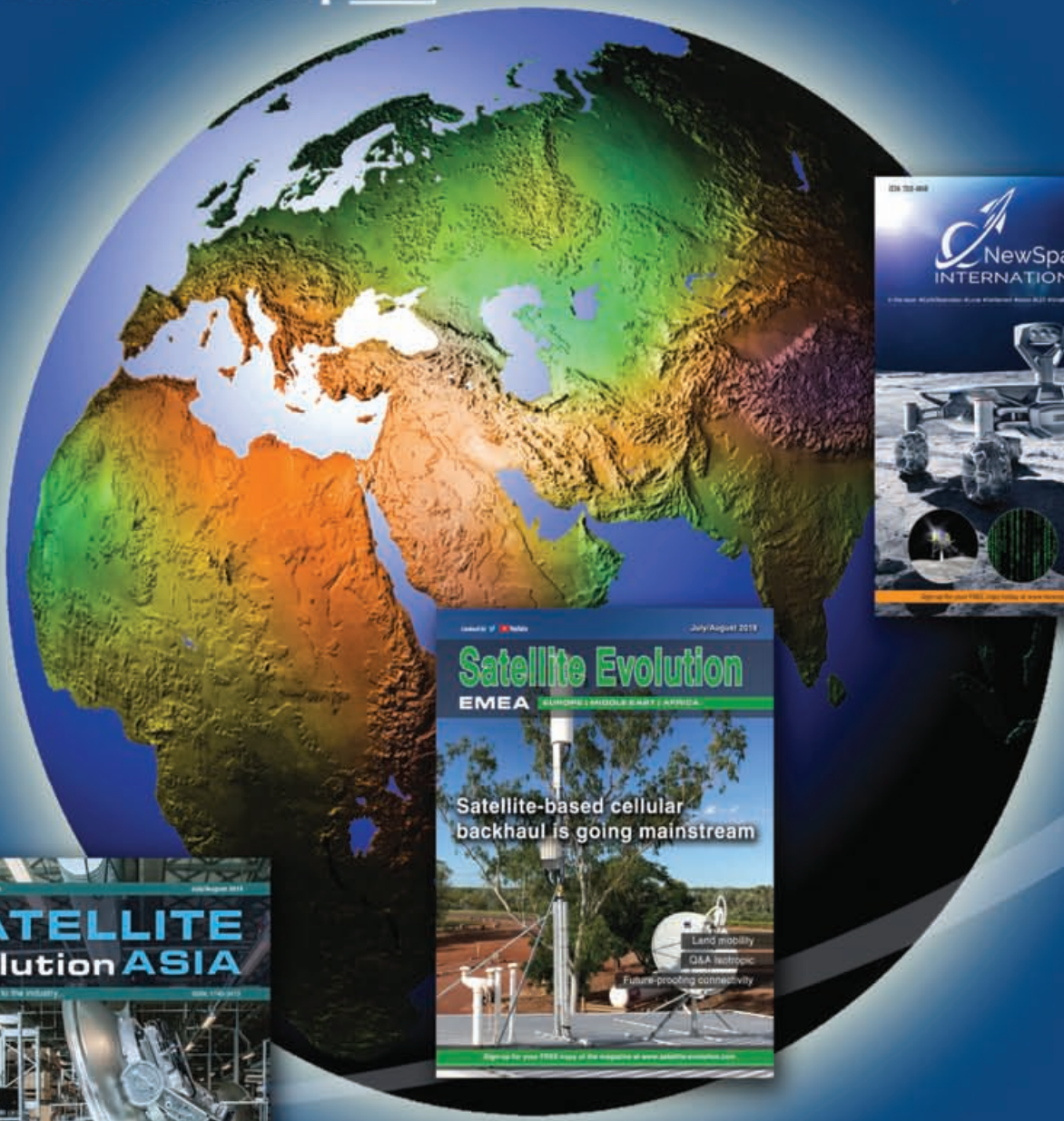
PACE isn't broken - It needs a different interpretation

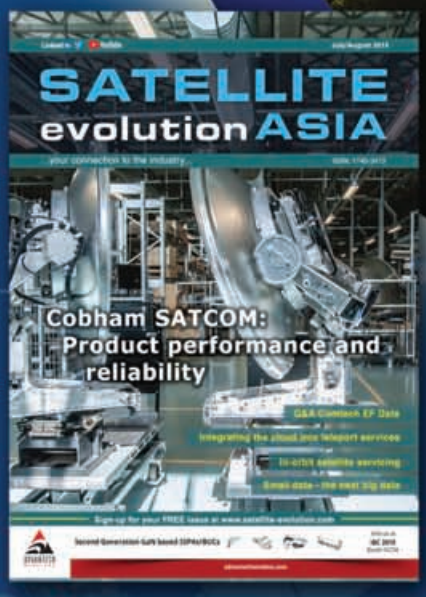
The above is an example of a PACE plan. All plans will be dictated on what is available, both from an equipment/system perspective but will also be driven by communications infrastructure available in the theatre of operations/exercise.

Even with time and effort invested in a PACE plan, forces are likely to find that the alternate system will be inferior to the primary system and the contingency and emergency systems will have questionable levels of security associated with them.

However, PACE is not about providing four levels of failproof communications, it is about assuring communications and keeping personnel safe in what can be highly hostile environments. It gives commanders the peace of mind that if all else fails there is a solution at hand that can be relied upon to maintain a link and empower personnel to continue with the task that has been set or in a worst-case scenario, simply survive. **GMC**

SATELLITE
Evolution Group





www.satellite-evolution.com

...your global marketing platform