



Photo courtesy of Glowlink.

The interference issue

Mitigation of interference on the battlefield is an incredibly important aspect of military communications. Helen Jameson learns more about the problem in an environment where interference could mean that lives may be endangered.

Military operations today are conducted in an environment that is increasingly reliant upon frequency and the electromagnetic spectrum (EMS). The devices used in the battlefield rely upon this for intelligence, communications, navigation, sensing, information dissemination, and for many more services. The EMS has enabled great advancements in the way troops and commanders communicate with each other and has led to the creation of a networked battlefield where technology takes the lead and can connect all echelons of the military. However, these incredible benefits are also balanced out with many risks and vulnerabilities. Electronic Warfare or EW is one of those threats.

Electronic warfare can be defined where electromagnetic energy, directed energy or anti-radiation weapons are used to attack personnel, facilities or equipment with the intent of degrading, neutralising or destroying enemy capabilities. The purpose of EW is to deny the opponent advantage in the EMS through interference that

can be inflicted from the land, sea or air and also in space by either manned or unmanned systems.

EW is often used to support military operations involving various levels of control, detection, deception, degradation, protection and destruction. Attacks on satellites result in the loss of critical information to those who need it most.

Interference can be placed into two camps – intentional and unintentional. Any interference can be considered a potential threat. Causes can be intentional or inadvertent, military or civil or foreign or domestic.

However, militaries can be their own worst enemies in terms of interference as they do occasionally interfere with their own systems due to user error and operation and procedures. In fact, the majority of satellite interference is created by user error but the small percentage that is created with malicious intent cannot be ignored and therefore, interference is a perennially important issue for any mili-



tary. Space can easily become a battleground for this form of electronic warfare.

Any instance of interference must be reported, tracked and the geographical location pinned down and the source identified. Is it the enemy? Is it accidental? Interference detection is a bedrock of command and control and military communications architecture. Systems must be able to provide real time information so that the source of any interference can be stopped so geographical location and data analysis are vital. When experiencing harmful interferences the operator has to be able to discern whether the interference is caused by natural phenomenon or manmade sources. With natural phenomenon the operator can try to work through the interference or assign an alternative frequency but if he or she suspects manmade interference, they can check and act upon it.

Protecting space assets

The US Department of Homeland Security published a paper this year entitled the United States Positioning, Navigation and Timing Interference Detection and Mitigation Plan Summary that recognises the importance of interference mitigation to protect the GPS constellation. In the paper, the importance of interference detection and mitigation is underlined; 'This heightened recognition is the impetus behind efforts to plan and prepare for incidents of interference to those systems and provide guidance for the timely resolution of mitigation and interference events'.

How is interference detected?

Systems that can pick up and locate interference are invaluable to the system users. These convenient products can cleverly pick up interference and provide details of location and whether the interference is accidental or hostile.

All of this information can be retrieved on a laptop and can be monitored remotely as well. Companies have developed interference detection equipment specifically suited to military satellite communications. Here are some examples.

Glowlink

Glowlink has recently begun to monitor traffic carried on the new Department of Defense Wideband Global SATCOM satellite (WGS-1) using a Wideband Global Spectrum Monitoring System (WGSMS) that ushers in a new era of wideband satellite communications monitoring and control.

WGS-1, which went operational on April 15, 2008, is the first in a new generation of wide bandwidth DoD communications satellites and is the most powerful in its inventory for long-haul communications.

"WGSMS is the first system that is capable of monitoring the new WGS satellites. The system is used to routinely measure the spectral signature of more than 4.5 GHz of WGS bandwidth in just a few minutes," says Daniel Hannan, Chief of Wideband SATCOM Operations Support, US Army Space and Missile Defense Command/Army Forces Strategic Command. "WGSMS enables Wideband Transmissions Controllers to 'see' spectrum that is actually transiting all WGS beams, regardless of band, with a single monitoring system."

"The WGSMS is a sophisticated, globally deployed monitoring system designed and developed by Glowlink for the WGS constellation," says Michael Downey, Glowlink CTO. "It requires an impressive array of the latest advances in spectrum monitoring, interference detection, and signal characterization technologies, along with an overlay of wide-area networking, database, information display and information assurance infrastructure. Glowlink is gratified that it is able to pull all these off."

Glowlink is under contract to continue product enhancement and technical support for the WGSMS as the WGS network evolves and expands to meet the crucial tactical, strategic, and operational needs of the US and its allies.

QinetiQ

QinetiQ's advanced system, satID, identifies and locates the source of interference to satellites, typically to within ten kilometres and in a matter of minutes. By locating the transmitters of the interference, QinetiQ alerts governments, regulators and satellite operators to the source of an attack. Its geolocation service is already helping protect broadcasters and other satellite users from loss of service. US Department of Defense has purchased two total geolocation systems from QinetiQ.

QinetiQ has seen demand for its expertise increasing both with governments and commercial satellite operators. For military users, satID works by using two intercept stations to track the interfering signal both in the target satellite and an adjacent satellite, which will be close enough to receive some of the beam from the offending transmitter. satID uses this knowledge it gains about their velocity and position to pinpoint the source of interference.

If the interference is accidental, the result of faulty equipment, or incorrect operation of ground terminals, the groundstation causing the problem will be alerted.

Satellite operators and Governments can choose one of three levels of geolocation service from QinetiQ. They can purchase a whole system, enabling them to pinpoint sources of interference wherever and whenever they like. They can ask QinetiQ to bring its portable Fly-Away version of satID to their location to interrogate the problem. Alternatively, QinetiQ can use its own systems to provide a geolocation service covering Europe and the Far East.

ERA Technology

ERA Technology and Chelton Electrostatics (CEL) have developed leading-edge adaptive antenna control electronics to protect commercial and military satellite navigation receivers from interference or intentional 'jamming'.

With the current proliferation of satellite navigation receivers and their use in a diverse range of applications, these systems are increasingly susceptible to unwanted interference. This interference can reduce positioning accuracy or, in some circumstances, result in a complete loss of data.

Most sources of interference are terrestrial with significantly greater signal levels than navigation data received from a satellite. Although current navigation receivers incorporate protection measures to filter this out, there are still situations where this is ineffective defence. As a result, ERA and CEL have co-developed a Digital Antenna Control Unit (DACU) to demonstrate the use of adaptive array antenna technologies that solve this problem.

The DACU incorporates the latest digital receiver technology. The adaptive processor is based around state-of-the-art 1500 pin Field Programmable Gate Arrays operating at over 300 MHz. The DACU will be used in a MoD trial with an eleven element Controlled Reception Pattern Antenna (CRPA) to determine the effectiveness of the approach for a number of operational satellite navigation scenarios.

Dr Neil Williams, Technical Director at ERA, said: "This project clearly demonstrates Cobham's world-class electronics design and development capability and our ability to provide solutions to complex technical problems."

Overcoming interference

Nothing can eradicate interference although many improvements have been made by antenna manufacturers, for example, to help mitigate the problems that are caused by interference and manufacturers of detection and monitoring equipment are investing a great deal of money in research and development to increase the effectiveness and functionality of their products. Military communication channels are probably the most important the world over. It is crucial that these links are closely monitored to ensure that no hostile interference can have any effect. It is case of being vigilant and preventing the worst case scenario. ■