Satellite interference: A growing problem for the military?

Is satellite interference a growing problem within certain military spheres? Martin Coleman, Executive Director of the Satellite Interference Reduction Group, opines.

There are varying opinions on whether the state of RF interference in the military has improved or not. There are some who believe it has, on the whole, improved in the last 10 years, while others believe the situation has deteriorated. What is agreed upon, however, is that interference is an important issue, particularly as demand for bandwidth and services grows. Much of this demand will need to be met by the commercial sector which, from the military point of view, carries high risk in terms of resilience and reliability, but is more cost effective.

Having said this, the commercial sector has worked hard to reach a balance in terms of interference which, although a significant problem, remains manageable. As a result, there is a lot to be learned here. Interference in the military is a highly unique and multi-faceted issue; remember, to the military it is treated as a 'threat,' whereas commercially it is seen as 'disruptive.' So, what are the main challenges and what solutions are available now (and are needed for the future) to maintain secure and reliable military satellite communications?

The challenge of military interference

Almost everyone with a stake in the milsatcom sector will admit that the challenges facing military users and operators are completely distinct to those in the commercial satellite world. Chris Dunn, Consultant at 3SDL Ltd and former Specialist Education Manager, UK MOD, agrees that "it's bad enough when a commercial provider might lose their feed for say, an important sporting event. But some of the intensive and critical operations we do across the globe will ultimately fail without dependable C2. This could lead to quite catastrophic outcomes considering today's ever evolving threats." Interference within the military space is quite literally life or death.

Even from the satellite operator's view, military customers present a challenge as they are "subject to higher demands in service optimization, more efficiency on their satellite links (which requires high modulation schemes) and less interruptions for critical-mission applications," according to Ruben Marentes, Technical Advisor and former Director of the RF Operation Center at Intelsat Corporation.

Although instances of interference and jamming are extremely rare when using military X-band satcom, each instance has to be addressed and managed as if it were a hostile act by a potential adversary. Colin Neal, Spectrum Policing Manager at Airbus, says that "we adhere to the same process for any instance using Spectrum Monitoring and Geolocation Systems to characterise, locate and isolate the interference source quickly and efficiently."

Clearly, intentional jammers want to cause as much disruption as possible without detection, making it extremely difficult to firstly identify the cause of the interference, let alone solve it. In this case, prevention is often better than a cure.

But unintentional interference is still the key problem, especially when it comes to multiple countries and services operating in one region. Consider the number of satellite networks in use by the numerous coalition forces during the ongoing war in Afghanistan. In regions of high military activity involving numerous nations, things can easily become complicated.

Martin Coleman, Executive Director, iRG

According to Dunn, interference is very often "not adversarial or intentional, but can be genuine unintentional errors and 'frequency fratricide.' However, this is absolutely understandable in the current global environment where we often need to work with other countries' militaries and systems, utilising a vast array of different kit and on different parts of the spectrum."

Andrew Bond, Sales and Marketing Director of satellite RF distribution expert, ETL Systems, says "the unique environment in which VSAT's operate is one of the biggest challenges for the military." Very Small Aperture Terminals (VSATs) are widely used within this sector but according to Bond, "discussions at IRG workshops and events suggest that VSATs are one of the biggest causes of interference, or at least that is what many report." VSAT systems can easily be set up incorrectly and can cause serious issues on the satellite itself which "may go undetected. This is caused by a combination of poorer training and field experience, as well as more regular deployment and moving of VSAT networks in a theatre of operations," Bond added.

Naturally, with military staff in constant rotation, it is difficult to keep up with the necessary training and education to ensure staff are capable of using, installing and maintaining satellite terminals and networks. As a result, human error is very often a cause of interference.

On top of this, Neal adds that within the military "the variety of different operating environments brings the need for a wide variety of terminal types all with their own individual satcom link

Andrew Bond, Sales and Marketing Director of satellite RF distribution expert, ETL Systems

Chris Dunn, Consultant at 3SDL Ltd

Colin Neal, Spectrum Policing Manager at Airbus

needs. Each arm of the British Forces faces its own unique problems, the rotational nature of the roles and the restriction on numbers can mean that in some instances the maintenance of the satcom link, during certain periods, may not be the primary role for an individual. The assigned maintainer may have the qualification but not necessarily the hands-on expertise, he/she may have been trained but Skill Fade makes him/her less effective. This is where the satellite service provider can help by understanding the environment within which the operator is working, understanding the pressures associated with the responsibility of providing and maintaining that vital satcom link."

Interference naturally involves two parties, and so resolution requires communication and the sharing of information. Sadly, Dunn believes one of the barriers to effective interference mitigation in the military is a "reluctance to admit problems due to concern regarding security implications." Of course, it is entirely understandable that military users are protective of their operations. After all, as Dunn says, "there are justifiable apprehensions in admitting issues regarding interference, in concern for providing valuable feedback and intelligence to adversaries in the battlespace." But this does, however, limit the ability for those being interfered with (whether that's military or commercial) to identify the cause of the interference, significantly lengthening the time to resolution.

Within the commercial sector, Carrier ID (CID) has been a useful tool for identifying the cause of interference and quickening the resolution process. This has proved especially valuable in solving large VSAT burst-mode terminal networks. Unfortunately, given the reluctance of militaries to share their location with non-cleared personnel, CID as it stands, is not an applicable solution within the military. Having said this, there have been attempts to set up a special military-suitable CID whereby only the CID number of military terminals are available, as well as the satellite operator responsible. In the case of interference, the 'interfered' simply contact the satellite operator who are then responsible for contacting the military user directly.

Future potential for RFI

Marentes believes that the RFI situation has improved in the military space with "more and more services supporting military applications in commercial satellites than ever before" and satcom maintaining "reliable performance, at a competitive price and with a reach/coverage sometimes unavailable to other systems."

One example is the introduction of the Digital Payload in Intelsat Epic^{NG} satellites. Marentes explains that the digital payload allows new restoral and relocation options previously unavailable to Intelsat Operations. "For example, if a customer is experiencing RFI on a frequency where remote sites are operating then the RF Operations staff can command the digital payload to be adjusted and the carrier can then quickly move to a different frequency range away from the interference without the uplinker making any changes on their end."

Dunn is of the opinion that interference is a "growing issue for how we [the military] operate around the globe." He also agrees that the military is increasingly having to utilise commercial bandwidth due to demand for services across the world: "We now often have to contend with utilising whatever capacities, both commercial and military, that might be available to fore-fill our ever increasing and often rapid demand to enable our effective C2 networks."

This shared arena where, according to Marentes, "services are impacted by all types of interference," can make it difficult for military users as "not all customers have the same amount of resources to respond to unintentional interference and their lack of action can disrupt mission-critical operations."

Neal adds that "military satcom is protected by strict terminal certification, this maintains terminal quality which in turn improves link budget accuracy and minimises instances of any unintentional interference. Military grade terminals are often operating within harsh and unforgiving conditions and suppliers are usually investing significant amounts to maintain quality and robustness." This is not always the case in the less tightly-controlled commercial bandwidth sector, meaning a potential for more interference. He goes on to say that military users experience little adjacent satellite interference (ASI) within x-band (a band reserved for use by only military and government users), saying: "I think that is linked to terminal control, exceptional satellite design and the fact we do not have non-compliant operators on the satellites." This being the case, heightened interaction between military sectors and commercial sectors, within the Ku-band environment, could increase the likelihood of interference for military users.

Collaborating for the future

It is absolutely essential that milsatcoms are error free. Consider the ship at sea, the aircraft on a remotely engineered runway and the small isolated team on the ground, all waiting for the influx of usable data that doesn't arrive. The absence of that data may impact humanitarian efforts, the inability to patrol a no-fly zone or the relay of vital imagery, all of which could be linked to a possible loss of life scenario. Data and information sharing has never been more critical.

In the modern military environment, Neal says that "bearers for many military satcoms are provided by commercial companies, either directly contracted to or through third party providers." But Dunn says that this being increasingly the case could worsen the state of interference: "As our demand ever increases across the entire useful spectrum, often conflicting with commercial requirements, this [interference] may get worse." This means that the military world must work with the commercial sector, collaborating on interference mitigation strategies and being open to communication.

The commercial satellite sector is in a good place with

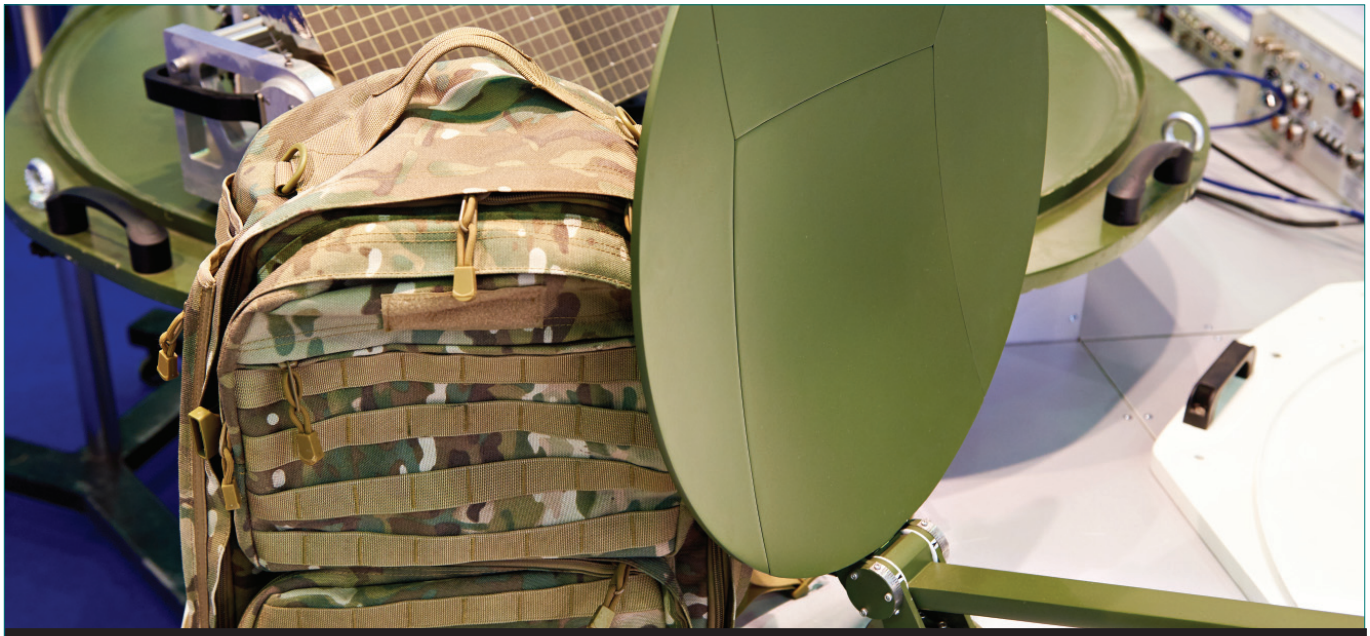

Photo courtesy of Shutterstock

regards to interference, as we are all aware commercial Ku-band providers/operators have had to deal with high levels of interference for years, and will likely do for years to come, so there is a lot that can be learnt from their experiences. At the same time, Neal believes if the military are planning to augment their military satcom capacity with commercial Ku-band (as an example) as a bearer "they should understand the limitations of their provisioned link and assess how this will impact the effectiveness of the operation, identify the processes adopted by the provider to mitigate the effects of interference and what visibility they will have of the incident. They must also impress on the service provider the level of support required not only during peacetime but also, if necessary, during a transition period and wartime." Clearly, the challenges of operating during wartime are distinct to those of peacetime, for example, the likelihood of intentional jamming by the aggressor and unintentional interference between allies in regions of high activity.

IRG, has, for a good few years, been the conduit between equipment providers, satellite operators and satellite users, a conduit through which ideas have been exchanged on the technical solutions to the interference problem. The group feels that it is well equipped and is willing to facilitate the conversations needed between both the military and commercial satellite sectors. Our relationship with both means that we can provide forums for debate and discussion and encourage the creation of new tools and techniques needed for interference mitigation in the future.

Photo courtesy of Shutterstock

Neal agrees that the military can learn from the commercial satcom sector by "maintaining a close watch on commercial satcom to see how it develops systems/processes to mitigate interference." The comsat sector has introduced several new solutions over the last decade capable of remotely monitoring, detecting and correcting errors that are equally as applicable in military scenarios.

Of course, it's equally as important to ensure better communication between allies in wartime, to prevent the possibility of 'frequency fratricide,' as mentioned by Dunn, and accidental interference. To this end, according to Neal, it makes sense to "maintain and exercise agreements with allies to share information, resources and expertise. An overall view of the spectrum and an understanding of the true impact of an unauthorised signal on not just your satellite may furnish the operator with the last piece of the interference jigsaw puzzle." It should be noted that the sharing of information is military to military, the commercial satcom provider operates, in these instances, as an information collector and possible solution advisor.

Similarly, allies should encourage one another to get on board with CID or at least a CID solution that provides its benefits in a secure manner. If we, IRG, the military and comsat sector, and other organisations could make a real go of developing a CID scheme suitable for all, we could make interference resolution possible by just picking up a phone. Many maintain that CID is not a solution for intentional jamming, but it does make it easier and quicker to differentiate between unintentional and intentional interference through a process of elimination. Working with the political influence of militaries, commercial satellite operators have a much better chance of being able to do something about jammers, too.

As Dunn maintains, we can ensure "rapid identification of potential interference, and then enable resolution of issues" through an "effective collaborative and secure feedback system." The military actually has a huge opportunity here, in terms of a shared feedback system.

Within the military there is a strict chain of command. All staff are tightly controlled and must record and report every occurrence of interference to command. In some cases, they even record how they solved the interference. With so much data on hand, it makes sense to use this data, potentially shared between allies, to build an AI/ML framework capable of analysing it and identifying trends and patterns. With this information, it could even be possible to predict cases of interference,

especially in the event of politically-motivated jamming (using information about events, cultural festivals, inflamed regions etc.). Although we don't have the technology capable of this yet, it has potential to overhaul the way we manage satellite interference in the military.

Of course, there are methods and technologies available to satellite operators with high throughput satellites (HTS) to limit the effects and prevent interference. According to Marentes, "having alternate paths," i.e. redirecting the satellite traffic to an RF segment away from interference, and "introducing error-correction schemes to the satellite links," can overcome most cases of interference. This works by intuitively adjusting the signal where there is interference in order to minimise its effect whilst maintaining the service at a lower quality. Although these methods may increase OPEX, it can create much-needed resilience in milsatcoms.

This flexibility however may not be possible. There are instances where satellite and ground terminal configurations need to be fixed, many nations are operating with systems that still require "nailed up bandwidth/throughput" so any form of Data/RF adaption is not possible, according to Neal.

Bond believes that where poor product quality is in evidence it must be improved, saying that: The best approach to interference mitigation is about "getting the right products in place to reduce errors." Poor product quality is a major cause of interference in the commercial sector and something many associations, including IRG and GVF, and operators are putting measures in place to prevent. Neal believes: "For the military, aging equipment and its supportability is the major source of unintentional interference, an issue that is difficult to resolve when many systems were built as one offs and are not commercial off the shelf solutions."

But if we improve the quality of satellite equipment, we must also work to improve the training given to those personnel that operate them. According to Neal, "training of users is the key to establishing, maintaining and recovering mobile satellite links." This is especially the case given the number of different terminals and services needing to be maintained within the military environment. Neal believes militaries should "look to provide varied levels of satcom training, not terminal specific training, [and] ensure within that training that the fragility of satcom is explained."

This approach would give military users, the people on the ground, a broader, in-depth understanding of satellite on the whole as well as an understanding of the implications of satellite interference and wider issues.

Conclusion

The military sector is unlikely to be able to meet the increasing demand for more and more services, and as such will have to rely on the commercial sector in a large number of cases. Given the future of LEO constellations, as well as ever increasing capacity in GEO for satcom, the military should be more proactive in considering the wide variety of commercial satcom that will likely be available in the future. This will offer flexibility and resilience across varied platforms and throughout the orbital regimes.

But of course, operating in the less tightly controlled environment of comsat could mean an increase in interference for the military. At the same time, both sectors have their own ways of dealing with incidences and there is a lot that can be learned from both. By collaborating on innovations and developments, and communicating information more openly, the military sector can make sure their use of comsat services doesn't impact operations. In my mind, it is about building an understanding on both sides of the fence and using the combined resources of the two sectors to bring about new technologies for interference mitigation. Most importantly, we must ensure interference is not 'out of sight out of mind.' With an increasingly congested and contested space domain looking likely in the future, it's time to put measures in place now to ensure error-free milsatcoms in the future. **GMC**

Photo courtesy of Shutterstock