A GetSat Microsat terminal fitted to the roof of a van via GRC mag mount. Photo courtesy GetSat

Keeping comms on the move secure

Comms on the move technologies answer the common and crucial demand of keeping operators in contact in remote environments and on-route to objectives. While a long-time requirement in military strategy, these heavy-duty communication links are being increasingly required in the commercial world in step with the digitization of industry 4.0. As airlines, transportation and shipping routes, besides countless government requirements seek always-online connectivity, the private sector stands to also adopt the much-needed cybersecurity of defence development.

Laurence Russell, Assistant Editor, Satellite Evolution Group

A recent product launch by Kymeta brought us the u8 MIL hybrid terminal, serving mission-critical applications with communications on the move (COTM) and networks on the move (NOTM) technology.

"For years, Kymeta's advanced technology has been a proven resource for mission-critical operations. Our new u8 MIL hybrid terminal is tailored specifically for military users, providing them with a rapid-deployment solution and the fastest out-of-the-box communication anywhere," said Bill Marks, Executive Vice President and Chief Development Officer of Kymeta.

The addition of the Kymeta Connect managed service offers reliable connectivity via a comprehensive, by-the-gigabyte package that utilises satellite and satellite/cellular capacity.

The release follows Kymeta's indefinite-delivery/indefinite-quantity (IDIQ) contract with the Department of Defence of up to US$950 million as part of their procurement efforts to produce systems supporting a unified force across air, land, sea, space and cyber domains to achieve what they refer to as Joint All-Domain Command and Control (JADC2).

The new reliability and power of Kymeta's u8 hybrid terminal serves a very apparent demand. Modern COTM does more than communicate; mobile connectivity in contemporary terms often means remote computer access, real-time imaging and video transmission and voice recognition commands. Perhaps one day it'll evolve into even more unrecognisable forms, rendering networked augmented reality overlays to grant operators unthinkable new insights into their objectives and environments.

While a term popularly associated with the military, COTM is now becoming more relevant to industries and consumers. The In-flight connectivity (IFC) markets, opportunities in the rapidly digitising maritime communications industry, as well as the hotly anticipated business of connected car and autonomous vehicle services are just a few of myriad opportunities to connect the world of moving devices.

Mission-critical civilian communications

Plenty of mission-critical technologies are required by the commercial sector, and not just with respect to emergency services, disaster response, non-governmental organisations (NGOs) but also various critical infrastructure providers.

Key transportation, civil service and utilities services worldwide, on the move or otherwise has seen fit to access mobile connectivity with mission-critical reliability. Of course, the expansion of endpoints that comes with widespread digitisation has its drawbacks, incurring conversations around cybersecurity.

Commercial and civilian sectors, particularly those of critical infrastructure are also perfectly suitable – if not preferable – targets of powerful cyber-attacks. As these bodies digitise to the standard of every other organisation in our time, they represent prime targets for bad actors, whether they be stateless meddlers or deliberate interference by unfriendly intelligence services. Needless to say, cybersecurity cannot be compromised.

Many UK residents can remember the Ransomware attacks on the NHS in the summer of 2017, which resulted in such chaos that non-critical patients were turned away by the crippled hospitals. It was widely reported that the healthcare service had been so poorly funded that thousands of computers in 42 separate NHS trusts were still using Windows XP.

This is to say nothing of the multiple breaches of US systems by what have been identified as Kremlin-affiliated cyber actors, who have targeted power, water, aviation and government facilities in addition to small commercial facilities since 2015. The UK's 2020 'Russia Report' lists similar invasions, describing Russian interference in UK politics as

Craig Miller, President of Viasat Government Systems

'commonplace.' Given the difficulty that comes with identifying the origin of a cyberattack, commentators have suggested the incidents that the Pentagon is aware of could well be the tip of the iceberg for Russian cyber interference.

With the fifth domain becoming ever more advanced in a world wholly unprepared for it, we must begin taking cybersecurity in industry and critical infrastructure ever more seriously.

Craig Miller, President of Viasat Government Systems, told *Satellite Evolution* that he believes that his company could be part of the solution. "Viasat possesses all manner of DoD-certified infrastructure customers on our network benefitting from government-standard cybersecurity. I think we're only going to see more of that happening as cyber gains prominence: Governments partnering with industry to develop best-of-breed solutions supporting comprehensive measures to protect what's important."

Defence technology for the commercial sector

Defence procurement is increasingly looking to commercial providers to develop their equipment, just as traditionally military developers move their portfolios into commercial markets. Mobile communications are set to be a big part of this new paradigm.

"One of the most interesting aspects of military technology in the 2020s and 2030s is the expansion of autonomous systems on all sides. That means the demand for comms, sensors and actuators are set to grow. Machines that see and do," explained Viasat's Miller. "These machines need comms to work, and networks to work well. The big data we can predict will be generated from a hypothetical information-age conflict would require a lot of heavy lifting. It's the kind of complication that'll take a suite of new technologies from the commercial edge that aren't currently thought of as part of warfare. Comms on the move will stitch those near-future systems together."

On the subject of the security risk of industry digitisation multiplying endpoints, Miller explained that "While a moving endpoint is no less secure than a stationary one, comms on the move technologies do increase your attack surface, because as you integrate more nodes, you increase the endpoints with which to access your network. Of course, access is the easiest step for hackers, and a lack of entryways into closed systems has not been a strong deterrent.

"That's exactly why we've seen a change in cybersecurity philosophy. Designers now work harder to consider threats that are already in the network. Bricking over your front door and windows when you know you've got a backdoor and skylight isn't the most practical strategy. With cyberattacks as sophisticated as they are, we need countermeasures to secure us at every level, not put another padlock on the access points we keep seeing them get around. The expansion of connectivity is inevitable. Cybersecurity needs to evolve beyond the threadbare strategy of having fewer endpoints."

Miller went on to recall how Viasat's cybersecurity successfully contended with the Mirai botnet, a disruptive malware first identified in 2016, when it struck their partners' networks. These were 'zero day' intrusions that ripped cleanly through an unforeseen backdoor, ignoring any and all conventional access points, which were mitigated thanks to reactive cybersecurity. "When you design with the assumption that everything is compromised, your architecture becomes a more flexibly performing combatant in crisis. It won't run out of moves and roll over when you hit DEFCON 1. It fights to the last line of defence."

Prioritizing holistic systems

The security of our communications networks both at the defence and civilian cutting-edge is likely to increasingly progress in tandem. The Internet is borderless. The front line against black hats and hostile states is drawn around your work laptop as cleanly as it is around the White House. There is no line separating defence and commerce in cyberwarfare.

But we must shirk the anxiety that exponential growth in COTM systems is expanding vulnerabilities. Cyberwarfare was always going to present significant risks, no matter our attack surface. We simply need to prioritize holistic cybersecurity systems and best practices to take these threats with the seriousness that they are warranted. ■

The u8 MIL hybrid satellite or cellular terminal is low profile, multi-orbit multi-network (GEO-LEO) ready, and easy to mount on vehicles and vessels. Photo courtesy Kymeta