Mark Patrick and Charlie Kawasaki

A Networked Battlefield – ISR Challenges and Solutions

Faster communications and continually connected devices, in the form of 5G and ubiquitous devices connected in an IoT infrastructure, will significantly change our domestic lives. Or so we hear during the commercial breaks between news segments or read in the Sunday papers over coffee. But is it just about faster data communications – or is there more at play and does this have ramifications for warfare preparedness? It turns out that there is much more in common between the race for supremacy in consumer and commercial communications and processing capability and the race for overmatch in the future battlespace.

Curtiss-Wright PacStar 453 GPU-enabled small form factor compute module with Digital Barriers' SmartVis server. (Photos: Curtiss-Wright Defense Solutions except where otherwise stated)

Before exploring the technology, it is worth reflecting on the changing battlespace. Urban environments are a key focus of preparedness as we further modernise – some would say *'futurise'* – our capability. Urban environments are complex to navigate, provide a myriad hiding placings and make asymmetric disruption and warfare harder to overcome from a planning and logistics perspective. Urban environments present a more complex signals challenge – both naturally, due to reduced line-of-sight ranges, and because of active measures to deny and disrupt communications, a tactic of both near-peer and asymmetric adversaries. Measures to overcome network attacks typically reduce the bandwidth available for communication and reduce the number of simultaneous broadcasters and receivers over that bandwidth – devices are essentially forced to go quiet. In planning our networks, we must therefore assume and counter this threat. In ideal conditions, bandwidth and communications concurrency is high, but our systems must still perform when bandwidth is low or intermittently interrupted.

Urban environments need more sensors for effective reconnaissance and early-warning surveillance systems because of the significant environmental clutter. More cameras, more motion sensors, more signal interception devices and more threat triggers, such as biochemical warning systems. Almost everything has the capability to become a sensor and to report its current status to processes that care about the environment the sensor is experiencing. A weapon may be a sensor: its magazine an independent sensor; a med-pack a sensor; what does the rifle scope capture before and after a round is fired? What is the current ammunition load on a solider, and is replenishment required? What blood-pack was administered, and does the field medic need new supplies or evacuation support for a wounded team member? Video is also of direct value to combat troops for quick planning decisions, to increase their safety and maximise mission effectiveness. Designing architectures that give rapid but secure access to local assets is critical.

(Photo: Digital Barriers)

Mark Patrick is Senior VP, Americas, for Digital Barriers.

Seeing is Believing

Video is by far the most demanding application of bandwidth and, increasingly, our militaries are projecting significant benefit derived from solider-worn systems, vehicle cameras, UAS camera systems and rapidly emplaced-overwatch cameras. This benefit comes with a price; a single high-definition camera can easily consume 3-5Mbit/s of bandwidth and, importantly, this is *uplink* bandwidth. Networks are often designed with asymmetric transmission capabilities, with higher download or 'push' speeds than upload or 'receive' speeds. A 3-5Mbit/s load for a single device is a heavy one to bear on a network – multiply this by hundreds of sensors and even the best designed military network is overwhelmed. Video data is also generally highly fragile, simplifying our adversaries' measures to disrupt its transmission, as a small number of bytes lost can break video transmission for ten or more seconds. Adding error recovery data into video for resilience can easily double the data bandwidth required, so this is

Charlie Kawasaki is PacStar's Chief Technical Oficer.

rarely a feasible option. Video is also poorly behaved on a network, because its data pattern is highly variable, with large peak-data spikes.

What is required is a more intelligent approach to how video is shaped for the battlespace, how it adapts to changing network conditions and how it is processed to provide actionable insight, without over-burdening central analysts. We need video data and auto-generated insight, delivered to augment human performance. The Digital Barriers approach is to reshape that video – both to reduce the absolute data bandwidth required, through more efficient encoding, and to remove the 'spikey' nature of video. This allows for significant increases in concurrent video streams in any portion of the network. Further improvements can be enabled, using AI processes deployed at the edge-device to determine what level of video fidelity is required, and what insight can be generated as meta-data to accompany the video. Or, these processes can remove the need to send video at all. This all requires an increased processing capability on which to execute.

Sectoral Cross-Pollination

A common pattern is emerging between commercial and military communications and processing needs; rapid innovation occurring in both sectors is creating bilateral crossover. To exploit innovation occurring in the commercial sector, our militaries need platforms that are compatible with the processing chains adopted in businesses that are driving innovation – particularly in intelligent network use and in AI processing. Innovation in the rapidly evolving commercial Video Surveillance as a Service market (VSaaS) is solving some of the challenges of a significant rise in wireless video. Advances in machine vision and processing for commercial security or self-driving vehicles are directly relevant to rapidly interpreting sensor data in the battlespace, and providing two greatly needed capabilities – rapid decision support and a reduction in wider network communications. These both require a step-change in the processing power available on or near to the combat zone, to prevent an overload of data moving through the network. This also requires higher-performance processors and, increasingly, Graphical Processing Units (GPUs), a technology created to accelerate gaming and now increasingly used to host AI-based processes. This is driving manufacturers such as PacStar to offer such processing capabilities on platforms sufficiently flexible and robust for in-theatre deployment, where more critical attention to size, weight and power (SWaP) considerations is required than in commercial settings. Placing data processing and advanced video compression on these platforms reduces data flow from lower to upper echelon networks.

Reducing data seems a curious goal, when we consider the commercial telecommunications space appears to be growing towards unlimited bandwidth availability. Even in this arena, however, significant technologies are brought to bear to minimise network traffic and to reduce data latency. Firstly, commercial networks cache data near sites of heavy use through content delivery network (CDN) technology – typically used to serve video to the home consumer. When that same data – a recently-released movie, for example – is requested by another user, the data no longer has to be retrieved all the way from the source storage: rather, a short number of network hops are needed. Advances in 5G also bring Multi-Access Edge Computing devices (MEC) close to the cell-tower, allowing data processes to be served on demand to data at its first hop from the transmitting system. Digital Barriers' systems can host analytic processes at the MEC, on the sensor or in a cloud service, depending on the processing capability available, data restrictions and required reaction time. This same architecture is directly relevant in the military domain, with analytics available on combat equipment, on local support vehicles or remotely at local and remote operations centres.

Reflecting on the changing landscape within the battlespace, and on the differences between commercial and military grade networks, leads to a number of observations and strategies to mitigate challenges:

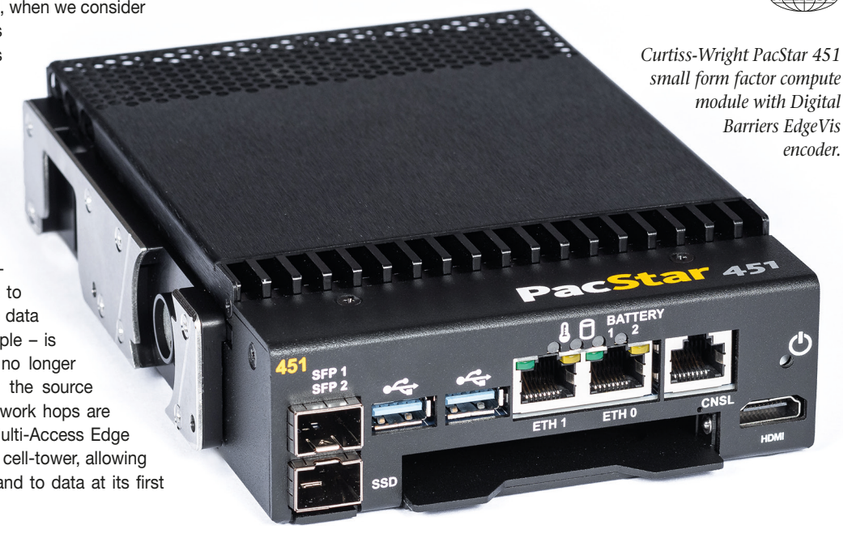
A sensor's data tends to lose value the more network hops taken before actionable intelligence is derived. Video data compression reduces fidelity in the video, losing detail for human and AI analytics. More hops increase time for end-to-end messaging, and increase risks of communication failure. The paradigm of moving data upwards in a network tends to lead to command intelligence, but not peer-to-peer intelligence sharing.

Data volume from sensors continues to rise faster than the networks capacity to carry it. A dramatic increase in the number and type of sensors is driven by the need to respond to near-peer technical development, and by complexities in the urban landscape. Additionally, sensors are offering higher resolution, which significantly increases data transmission rates. Networks, however, are under increasing attack, and strategies to mitigate this often reduce available bandwidth.

Military networks are inherently less reliable than their commercial equivalents. The inherent mobility requirements in warfare, coupled with the temporary nature of networks and with an adversary's attempts to disrupt and deny communications, leads to ever-changing communications availability.

All these challenges can be solved through designing flexible computing architectures – at each network tier – that intelligently process data as close to source as possible, and allow peer-to-peer sharing as well as careful management of data-flow between networks. The advantages of increasing video collection for intelligence purposes are too great to simply deny widespread use of theatre-derived video sensors, but new encoding and routing strategies are required to add greater adaptability to this key data.

Military strategists and communications programmes acknowledge that future overmatch on the battlefield will rely on information dominance and high situational understanding. While the proliferation of sensors and video sources has the potential to enable that overmatch, the contested RF spectrum and urban conflict threaten the ability to leverage those information sources. Using distributed computing and processing, with advanced AI for video processing and analytics, at the network edge, is key to making this possible.



Curtiss-Wright PacStar 451 small form factor compute module with Digital Barriers EdgeVis encoder.