



# ROUGH AND READY

**Fred Kao** examines the importance of harnessing technology to transform the military and defence sector

**R**ugged technology is revolutionising the military and defence sector as it continues to play a vital role in improving communication and productivity on the battlefield. This growing trend has led to an increase in demand for more sophisticated devices, but new warfare methods have also helped to shape its functionality and capabilities. Increasing situational awareness through digital application and advanced technology remains vital, helping protect forces and keep them one step ahead of the enemy. Cutting-edge technologies, including AI, new materials, 3D printing, big data and the Internet of Things are proving invaluable in securing technological supremacy. As these devices continue to offer a strong return on investment, we anticipate that demand will continue to grow.

Over the past year, increased aerospace and defence spending budgets across Europe has resulted in strong investment in technology and we expect to see continued spending across several territories in the year ahead to support digitisation within this sector. Innovation and digital transformation are shaping how military organisations operate with the most successful and dynamic investing in flexible, versatile systems and networks that improve their capabilities. Where customisation remains an essential asset to help protect forces, we are noticing the incorporation of 5G, artificial intelligence and new materials within these devices, allowing the military and intelligence agencies to harness big data, cloud computing and the Internet of Things. We also anticipate more emphasis on information technology integration for drone, real-time imaging, telemetry and surveillance applications to combat increasing hostilities. In

addition, organisations cannot underestimate the use of this technology to support disaster response and humanitarian efforts.

The deployment of 5G technology, the Internet of Things and artificial intelligence is revolutionising the rugged devices market, and the military and defence sector is leading this charge. Not only does this technology facilitate the smooth flow of data across all branches of the military, but also supports the safety of troops. For example, the sensing and computing devices worn by soldiers and embedded in their equipment collect various static and dynamic biometric data. The detail of the data collected from cutting-edge rugged devices can also be consolidated and analysed so it can be used immediately to help inform missions and courses of action for teams on the ground, including recovery operations. Rugged devices with 5G capabilities can transmit data and images from the battlefield, allowing military personnel to monitor progress and make informed decisions. Military organisations are also integrating robotics and autonomous systems (RAS) into their armoury and weaponry. Protecting troops, improving situational awareness and reducing soldiers' physical and mental workload while gaining ground on the battlefield are key objectives for military organisations. Beyond operational functionality, in the global race for AI supremacy, countries are competing to dominate this technology, recognising its significance for security and sovereignty.

The flexible and secure transmission of real-time data has never been more important to the military, and the latest cutting-edge combat information systems are transforming operations. For example, the SCORPION combat information system (SCIS) deployed by the French Army is putting data at the heart of the battlefield by allowing battle groups to connect and share combat information. This allows them to enhance combat capabilities and allow soldiers to quickly adapt to new operational challenges. This information system gives them real-time tactical superiority over the enemy. From the central command post down to combat vehicles, it brings combatants and weapon systems together, facilitating the transmission and sharing of tactical information. The flexible use of rugged hardware that forms part of the information system means devices can be deployed on military vehicles, including tanks and drones, which serve a control centre function to instantly share friendly and enemy positions via GIS maps. These rugged tablets can also be carried by infantry units, either on a chest mount or in a backpack, alongside radio equipment to allow a 360° view of the battlefield. Crucially, the versatility of this system means that the army can also interact with allied forces for greater situational analysis and operational planning. This information system is redefining joint combat and the digitised battlespace.

The rugged devices market has seen increasing demand for customised solutions catering to industry-specific needs. For example, some organisations require devices that can withstand extreme temperatures or hazardous conditions, while others need those with extended battery life – all of these requirements apply for the military. Today's devices can easily be expanded to become a portable cloud or local storage device or

server providing immediate and safe analysis, capture and analysis of data for accurate decision-making, such as GIS maps for mission planning. Plug-and-play expansion capabilities also mean rugged devices can be used as a remote control or radio system for automated technologies such as unmanned aerial vehicles, drones or other robots, or could be integrated with other technologies such as thermal imaging, heat sensors or night vision goggles. Aerial drones or unmanned aerial vehicles collect massive amounts of data from their journeys recording live streams for optimum surveillance or inspecting and monitoring mission zones. A central rugged device has the capacity to collect and process this data in real time to provide instant intelligence to teams on the ground. Beyond supporting tactical operations, the speed and agility of this technology can also be leveraged to reduce the human impact of warfare, supporting disaster response and relief operations and boosting humanitarian efforts.

## THE LATEST DEVICES CAN TRACK LOCATIONS IN THE FIELD AND FEED BACK TO THE CONTROL CENTRE

Military and defence organisations are constantly adapting their Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) strategies to improve efficiency, operations and decision-making. Adaptability is a core requirement of this technology, which must perform a range of tasks, such as asset management and repair, diagnostics and maintenance, logistical organisation, flight maintenance and mission control. Rugged devices have radically improved over the past few years to meet this need. Leading manufacturers are producing laptops and tablets that focus on size, weight and power (SWaP), producing smaller, lighter and more intuitive systems. However, this new SWaP focus doesn't mean compromising on performance. Command control systems (CS2) require increasing levels of computing power, so the latest computers still pack in more power for an uninterrupted performance on and off the battlefield. These devices need to operate in all conditions, from sand and snowstorms, to rain and extremely high and low temperatures, all while withstanding drops, knocks and spillages that come with the territory. To meet this demand, modern rugged devices are tested to the highest standards and include both MIL-STD and IP certifications. The latest computers go beyond even these benchmarks, ensuring continued function in explosive atmospheres or where there is solar radiation, salt fog or fungus. These cutting-edge tablets and laptops, for example, incorporate seamless design and fanless functionality for extreme resilience, robustness and durability in even the most uncompromising environments.

The ability to safely access and transmit sensitive data while in the field is mission critical, so rugged devices must guarantee top secret security classification to protect against cyber hacks,

**Computers need to operate in all conditions, from sand and snowstorms, to rain and extremely high and low temperatures, all while withstanding the drops, knocks and spillages that come with the territory**

infiltration or other security threats. With increasing reliance on digital systems, safeguarding against cyber threats has become a critical focus, centred on securing networks, data and critical infrastructure

## 5G, THE INTERNET OF THINGS AND AI ARE REVOLUTIONISING THE RUGGED DEVICES MARKET

Devices should include the latest version of UEFI BIOS with secure boot protection and a trusted platform module (TPM), which protects certificates and RSA keys for hardware authentication and FIPS 104-2 compliance – mandated by US and Canadian governments and generally accepted worldwide – which means the device has been validated for effective cryptographic hardware. This level of flexible connectivity and advanced wireless capability allows soldiers to communicate whenever and wherever they need to, allowing instant access to data and information and using mobile communications in real time for enhanced situational and operational circumstances. The latest devices are part of the ‘modern’ soldier’s equipment and can be used to track locations in the field and feed back to the control centre. More importantly, high-speed voice and radio-activated transmission systems

operate with military satellites to enable the secure exchange of large flows of data, while preventing EMC emissions over a given geographical area. Other important security features that can help minimise the threat of a cyber attack include: personalised identification and authentication via fingerprint and smart card readers and RFID. It is also essential that storage devices can be removed easily and rapidly in case of an emergency, so that data can be protected away from the device.

As modern technology continues to advance, we expect to see rugged devices that are smarter, more efficient, and more reliable coming to market. Innovation and digital transformation are shaping the way organisations operate across every industry worldwide, but nowhere is this more prominent than in the military and defence sector. The most successful and dynamic organisations are investing in flexible and versatile systems and networks that improve operations and recognising that this is where investment is most beneficial. While speed and agility is critical, the growing risk of cyber warfare cannot be underestimated. The latest intelligence systems are designed to meet stringent military standards that safeguard data in every environment while simultaneously protecting troops and supporting humanitarian efforts. The most advanced rugged devices are revolutionising the sector and setting the pace for digital transformation that is changing the shape of warfare ●

**Fred Kao** is CEO of Twinhead International Corporation. Before being named CEO in February, 2010, he was Twinhead’s Vice President responsible for the global product planning, sales and marketing of its core brand Durabook.

**Cutting-edge tablets and laptops incorporate seamless design and fanless functionality for extreme resilience, robustness and durability in even the most uncompromising environments**



Picture credit: Durabook