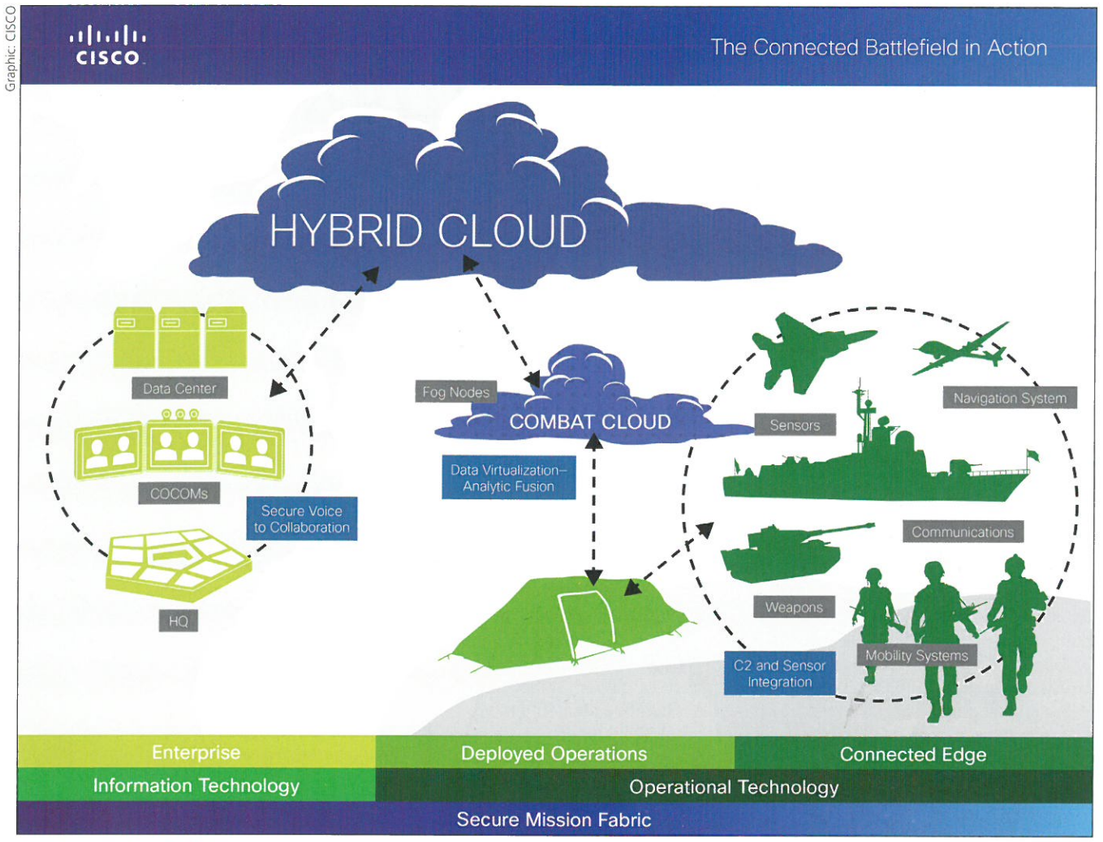
Graphic: CISCO



According to a CISCO vision, the "Internet of Everything for Defence" will pave the way for the connected battlefield of the future.

Other applications of dedicated networks would be used in support of large groups of autonomous robotic vehicles, whether land-based, aerial, or maritime. Employing a node to every unit in the swarm help set a mesh-like MANET, that extends across the entire area and airspace where the units operate, offering an autonomously managed, resilient network that is tougher to defeat, than a group of robots under human control. Autonomy is essential for such an operating architecture, as a human operator for each unit will not contribute to its operability but rather slow it down and make it more vulnerable.

Increasing the number of connections on the MANET presents significant opportunities and benefits, but also rising security concerns about unauthorised monitoring or seizure and control of critical-to-military operations.

An Opportunity and a Risk

Facing the high cost of dedicated military radio networks, military users have adapted commercial networks for peacetime operation, backup services, primarily for enterprise support of military operations.

Current military-commercial networks are based mainly on 3G and 4G LTE. Some of those networks, such as IAI's TAC4G employ hardened systems and nodes based on 'militarised' LTE. At the same time, SDR radios support waveforms tapping commercial networks where they are available, thus enabling defense applications to tap the bandwidth, availability, and commonality the commercial networks offer.

The next generation of networking, known as 5G, provides a quantum leap in performance compared to 4G LTE. 5G provides many of the advantages offered by modern SDR, namely MANET, Mobile-to-Mobile (M2M) links, and practically unlimited networking capacity supporting a fully networked cloud space and internet-based apps services.

5G providers promise that defense applications based on 5G technology will provide the 'missing link' to enable high-speed information aggregation, access, and distribution the military is missing today. They even defined a new term - Command, Control, Communications, Computing Combat systems Cloud (5G-C5ISR). Defense system architecture based on this 5G-C5ISR can harness end-point processing, big-data solutions, leadership information dissemination along with troop-to-troop, device-to-device, and user-to-system connectivity.

Despite the attractive benefits and affordability of 5G technology, the military has not yet embraced it, at least not for combat operations. Nevertheless, The US DoD considers 5G technology to support peacetime operations in the continental US and abroad, but retain dedicated to military networks for combat operations overseas. The US is wary of the potential risk of network and information vulnerability to foreign actors. Such risk may occur from the use of foreign technology in the system infrastructure or system operation that could compromise information and applications. The network technology can also compromise other networks that are connected to those compromised networks.

This risk brought the US government to pressure its NATO allies to ban using Chinese technology on their future 5G networks. This pressure failed to gain universal acceptance in Europe, as France and the UK approved Huawei to bid on local 5G networks.

From a Kill Chain to a Kill Web

With smart sensors becoming ubiquitous, the flow of intelligence and battlefield information increases, enabling military users to become more alert and responsive to changes and opportunities. Networked sensors and actors (a.k.a. effectors) are harmonised to support a faster, more effective and decisive action, implementing faster Observe – Orient – Decide -Act (OODA) loop, also known as 'kill chain'. Today, such capabilities are 'hard-wired' in dedicated applications, responding to strict operational rules of engagement and centralised control of the use of force. These procedures were dictated by western nations in the past 30 years of military superiority over asymmetrical opponents, fighting non-state and state-supported terrorists, guerilla in low low-intensity conflict.

After decades of force reduction to their military forces, the US and NATO cannot rely on their qualitative overmatch of the Russian threat. In the air and on the ground, NATO and the US military lack the combat-ready Order of Battle (ORBAT) both in quantity and agility, to concentrate the assets needed to defeat a decisive, deliberate attack. A preemptive offensive move against the air and missile defense would also be costly, as the current doctrine requires extensive support and strike packages to pave through the enemy Anti-Access Area Denial (A2AD).

With uncertain air support, land forces move to obtain new capabilities that can respond quickly and decisively against opposing forces. Different forms of unmanned and autonomous platforms and weapons offer such capabilities – in the form of individually controlled loitering weapons, drone swarms, and smart, guided weapons. Such platforms carry sensors, information processing, commlinks, and weapons.

To effectively operate these weapons, two levels of communications are used, forming a 'Kill Web'. One is the inter-drone network that links multiple autonomously operated platforms and smart weapons, to act in unison toward a common goal. A higher level of control links the human operator with the kill web, providing overall control of the entire pack and attack of specific targets. A Kill Web enables users to quickly deploy these capabilities, rapidly group to locate and attack the enemy's weak point, and asses the level of damage inflicted.

Securing Data and the Cloud

Part of the cloud's resilience is the protection of the information that goes in and out. Facing a growing risk of cyberattack, sheltering behind firewalls is not sufficient to protect the entire system and the information that flows through it. According to Cisco, protection of the modern Internet of Everything (IoE) complex should extend to the tactical edge by employing a new, distributed computing environment known as the Fog. According to Cisco, Everything must be secure from the sensor and information it provides to the end-users on the Fog and the data center on the enterprise cloud.

Applying security measures to sensors and devices requires encryption at the point of aggregation. This is applied either within a 'smart sensor', or its associated 'smart modem'. Both require adequate storage and computation for encryption.

The Fog - the new distributed computing layer that closely couples sensors, devices, analytics, and end-users at the battlespace, enables the evolving operational doctrine of distributed control. This Combat Cloud and its Fog Edges must be secured to ensure data integrity and protection throughout the data lifecycle. It delivers the ability to collect, aggregate, and manipulate data locally and securely connect to enterprise and cloud repositories for further analytics and use.

When deploying modern military information systems, connectivity and security go hand in hand, to ensure every user can deliver and access information instantly and securely. Security measures must protect the entire data chain. Once secured at the data source and fog edge, security, and protection must maintain an unbroken trust from the source, through the intelligent network and into data centers. Similarly, information must be secured when distributed, replicated, and manipulated by lawful users. As military operators wait for those services to mature, system architects have a long way to go to win their trust. ■