ARQIT

Quantum Warfare and the 21st Century Battlespace

Quantum Warfare and the 21st Century Battlespace

The 21st Century Battlespace is a place of unparalleled complexity and technologically driven change. The advent of capabilities previously unimaginable to a war fighter outside the realms of science fiction are now manifesting at a phenomenal pace and scale. Allied Nations are finding it an increasing challenge to maintain 'innovation at the speed of relevance' whilst mitigating the access by adversaries to openly available 'levelling-up' technologies.

Innovation in the digital domain has underpinned some of the world's greatest technological leaps of the last 20 years and this is only accelerating. The corollary to this, is an increased focus on cyberspace and protection against digital aggressors – and the advent of 'Quantum Technologies' will see another step change in this dimension.

Maintaining an information advantage is now as important as raw numerical force levels or sophisticated technology overmatch. The adoption of cutting-edge commercial technologies, fused with more proprietary capabilities, whilst denying an enemy the ability to penetrate or disrupt such hybrid networks is part of a new capability development paradigm.

Data is increasingly being treated as a new weapon system, and access to it is now as important as fuel and bullets to the modern war fighter. Such access needs to be automated, interconnected and interoperable across multiple domains globally. It requires machine-to-machine as well as human-to-human and human-to-machine interfaces of unprecedented scale and connectivity and needs the security architecture to match this.

Joint All Domain Command and Control – Securing the hyperconverged edge

Joint All Domain Command and Control (JADC2) describes a US Department of Defence ambition to revolutionise the military's command and control (C2) infrastructure by establishing a combined, synergistic network of sensors, data sources, cloud architecture, software enabled and shared via wireless connectivity. It will deliver, collective, real-time decision-making across the Air Force, Army, Marine Corps, Navy, and Space Force, across land, sea, air, space, and other warfighting domains.

It describes a model to collapse traditional stovepipes and legacy architectures and create a fused, multi-nodal, multi-domain C2 capability with a fundamentally different approach; leveraging Cloud, Open Standards, Edge Compute, Software Defined Networks, 5G, AI, ML and an array of other emerging technologies.

The US is not alone in its ambitions, and many of the worlds more sophisticated militaries are deep into consideration of similar concepts.

Historically the US and NATO allies have relied upon a comparative advantage in technology versus even their most advanced adversaries. With the advent of large-scale low-cost 4th Industrial Revolution (4IR) technologies available to all, as well as recent heavy R&D investment by some notable adversaries, this advantage has been eroded and, in some cases, reversed.

The next generation advantage will be underpinned by access to rapid data driven decision making, allowing militaries to outthink and outpace even their more technologically sophisticated opponents. Sophisticated proprietary systems of the last decade are now themselves a limiting factor in the increasingly interlinked, data rich environments of the 21st century. It will see a move away from the reliance on closed networks, with data-bricks, manual encryption fills, and hardware based black-box security. Instead, the JADC2 paradigm shift, will turn to common platforms, open standards, and a need for a new model of security and cryptography.

> *"We have to be able to trust data, and when people can break the encryption, that's a huge problem."*
>
> **General Stephen "Seve" Wilson**

But it is not just existing assets that will need to be brought into the 21st century and networked with one and other. New capabilities will not be able to operate at scale within closed, proprietary architectures. Drones, autonomous platforms and real-time data feeds, delivering a Common Operating Picture down the Tactical Edge with AI supported automated decision making, all drawing on a massive, dispersed Internet of Military Things (IOTM) will be the driving force behind a revolution in military affairs. Features within JADC2 will include:

- Data driven decision making, drawing on numerous data sources and multiple classifications with machine supported analysis to shorten the information cycle
- Cloud enabled end points, compute at the edge, multiparty accessibility
- Access to a multitude of different connectivity bearers from proprietary secure radio, to 5G and space-based mesh networks
- Manned and autonomous machine interaction requiring dynamic multiparty interoperability

Amongst the biggest challenges for this step-change will be the security of such networks, as well as the permissions of data access, authentication and the need to enable joint, and coalition partner interaction. The fundamental security of the encryption layer is of paramount importance – the world needs stronger, simpler encryption, and recent publications by NIST and the American Presidential Executive Order on Improving the Nation's Cybersecurity were powerful calls to action on this. But the ambitions of JADC2 cannot be achieved without the flexibility to securely vary sharing permissions to synchronise in real time with mission changes across multi domains.

Security in the hyperconnected era

A move must be made beyond the point-to-point 'hard security' of a relatively limited number of interacting assets, to the adoption of a more dynamic, cloud-friendly model, operating at hyper-scale. Symmetric keys have for a long time been a preferred way to protect mission critical data feeds, but they need to be able to form, and re-form in a more organic and high scale manner. The trust layer must be extended to a vast number of new endpoints. Secure processing at the edge means safeguarding that information in the environment in which it is being generated and managed, which is now as close to the data sources as possible. Hard-link encryption systems designed for a data in transit security model may no longer be as appropriate for the next generation of network topologies and data security needs to exhibit new characteristics of agility and fractional permissioned access. The answer, however, cannot realistically be to rely on conventional, commercial, cloud enabled solutions, leveraging well understood architectures such as Public Key Infrastructure (PKI). For all its dynamic interoperability benefits, PKI creates unacceptable security risks, particularly in a post-quantum world, that a military user will be unable to tolerate for anything mission critical. What is needed is a way to extend the Symmetric Key distribution zone to meet the new paradigm within JADC2.

Arqit's QuantumCloud™ provides a highly scalable method of mitigating many of the fundamental security challenges. QuantumCloud™ is a drop-in alternative for network security that addresses the shortcomings of PKI and delivers a host of new benefits to customers today, as well as protection against the coming quantum attack vectors. As a cloud-based symmetric key platform, it is easy to scale and allows users to concentrate on practical security outcomes within the rest of the network stack without worrying about the underlying encryption layer.

QuantumCloud™ provides an efficient way of distributing symmetric keys. It replaces the relatively unsafe Diffie-Hellman with a trustless broker-based architecture where the broker is used instead of a hard mathematical problem to allow the two parties to agree a key.

QuantumCloud™ and its automated key-fill process (ATK) solves the problem of key distribution for end-to-end encryption without the use of PKI by enabling existing symmetric key protocols such as AES256 to protect every part of the network without the need for change to the standards.

QuantumCloud™ facilitates a number of crucial enabling features which brings the JADC2 vision to life:

- Computationally secure symmetric keys can be created by every network component “over the air” and in a trustless manner in real time.
- Groups of network components can create group keys of unlimited size and frequency of change which can be reformed to eject or admit components from/to the group.
- Keys can be changed within seconds at low cost and without the manual rekey process overhead.
- Symmetric keys are already approved and are consistent in proven common network standards.
- High interoperability - collapsing security layers to provide effortless segmentation and user defined, permissioned access to multiple security enclaves in a dynamic and tailorable manner.
- The movement of data without the legacy stove piping, but retaining the authentication, control and security that such systems still require.
- The enablement of a new dimension of battlefield assets, from unmanned platforms to 5G/6G networks, IOMT and AI/ML processes.

The QuantumCloud™ platform can be incorporated into existing architectures via software interfaces, operated through secured private instances inside defence environments, and enabled by a sovereign global satellite network as part of Arqit’s Federated Quantum System (FQS) concept.

“We’ve already seen China declare quantum supremacy, and their purpose is quite clear. But in Arqit’s mission I found a solution to frustrate our competitors.”

General VeraLinn “Dash” Jamieson

Conclusion

The military and government ecosystems of the 21st Century will increasingly be data-driven interoperable, networks-of-networks that require a security layer that reflect this hyperscale architecture but more importantly match a changing threat landscape. QuantumCloud™ is a vitally important tool in enabling the delivery of this and other capabilities in the coming Quantum Age.