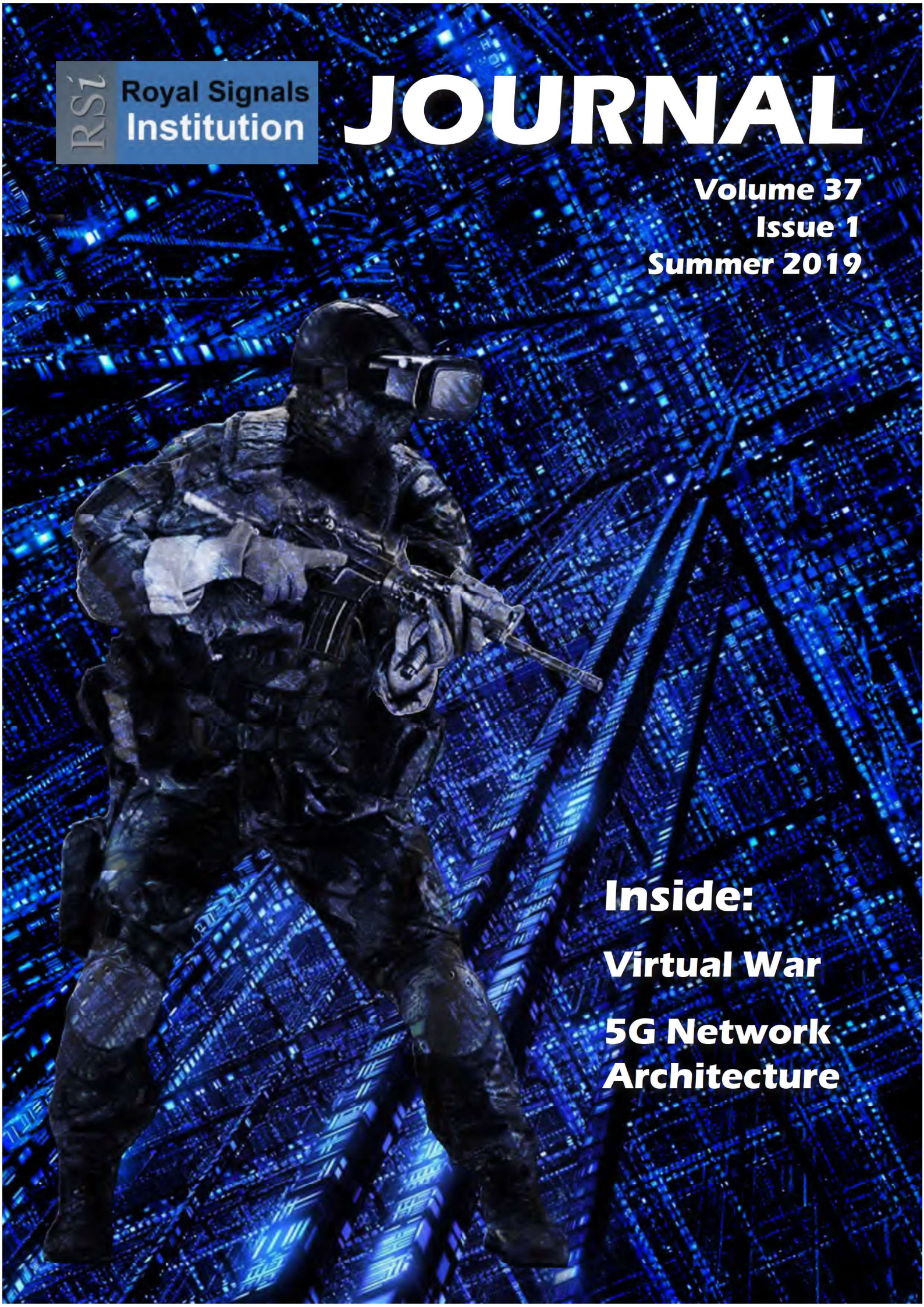
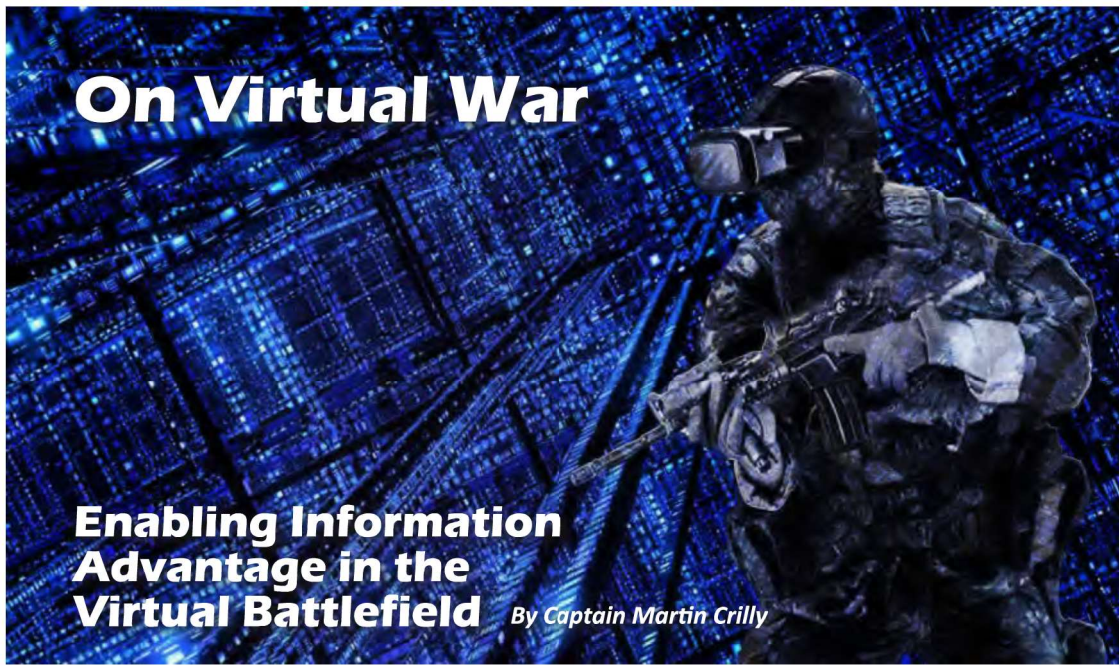

RSI
Royal Signals Institution
JOURNAL
Volume 37
Issue 1
Summer 2019
Inside:
Virtual War
5G Network Architecture

On Virtual War



Enabling Information Advantage in the Virtual Battlefield

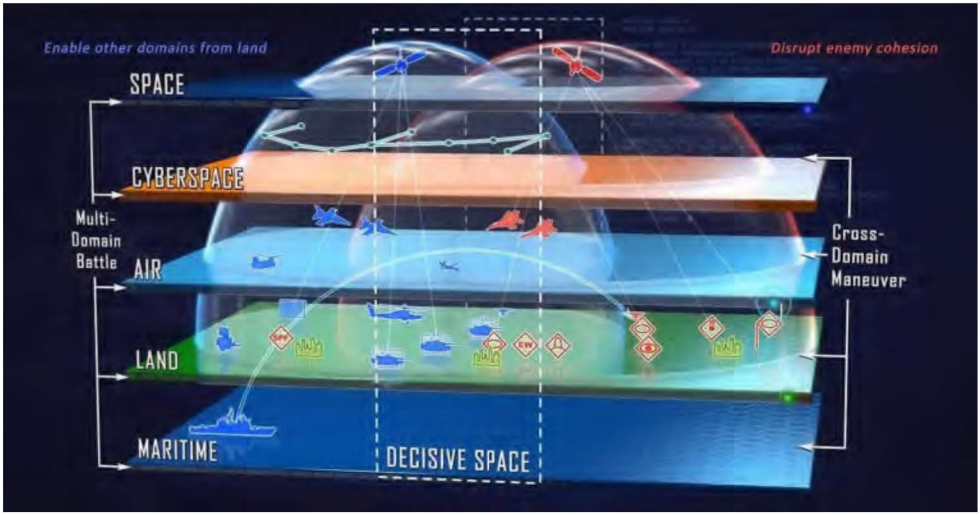
By Captain Martin Crilly

To win wars in the Virtual Battlefield, Defence will need to deploy modern hyper-scale computing to the Battlefield to enable solutions at pace to problems not yet envisioned.

1. The Virtual Battlefield

The contemporary explosion in computing power, the paradigm shifts in social communications and rapid socio-economic changes affecting global society are disrupting our military construct. They are transforming the traditional linear battlefield into the new multi-domain *Congested, Cluttered, Contested and Constrained* [1] virtual battlespace. For a Military and its Signals Corps to have relevance in this Multi-Domain Battlespace (Figure 1) and 'the grey zone just below the threshold of conventional warfare' [2] it needs to replace its 20th Century Industrial Age CONOPS to compete in the new interconnected multi-domain war. To wage today's war, a modern military will need to be capable of deploying an array of Virtual Warfare weapons / enabling systems, build competencies in its people and develop a 21st Century Information Age CONOPS that will shape the way we enable the full spectrum of influence across all domains.

Figure 1 Today's Multi-Domain BattleSpace - Congested, Cluttered, Contested and Constrained [3].



'The nature of persistent state-on-state competition continues to challenge traditional, linear crisis response command and control processes and structures. Defence, therefore, requires an applied operating concept, doctrine and new approaches for command and control to reflect a multi-domain, full-spectrum approach' – JCN 2/17 [4].

The character of warfare in this multi-domain battlespace is also changing: A new 4th generation hybrid warfare, a grey proxy style of virtual conflict is now blending all the different generations of warfare with today's contemporary technologies. This hybrid pseudo-war is playing on society's omni-reliance and addiction to instantaneous data feeds and all-pervasive social networks. The next generation of information tools, influencing physiology and integrated interoperable systems now require a new emergent Virtual Warfare doctrine. This is needed to enable future military forces to receive, analyse and comprehend contemporary battlespace data feeds in real-time. This can only be achieved by the integration of contemporary technology roadmaps, competencies based on the Skills for the Information Age (SFIA)[5] framework and new Information Age doctrine developed from the tech industry then applied in today's battlespace. Welcome to the Virtual Battlefield.

2. Virtual War stratagems

The enablement of Virtual War falls into 3 inter-connected Digital Transformation (Dx) stratagems;

1. **Informationisation:** Everything is to be digitised into big amounts of data, collected, transported, stored and processed into information;
2. **Intelligentisation**: Information is to be analysed into intelligence; and
3. **Cognitivism:** Sense is to be made of this intelligence to enable (and automate) decisions and actions.

'The most successful people in life are those who have the best information' - Benjamin Disraeli

Informationisation describes the practice of embracing all the technological opportunities of the Information Age and integrating them into military planning systems. In Virtual War, a commander will likely have access to 1000s of separate digital data feeds and all of it available in their deployed HQ. Data endpoints at the network edge, eg Ajax with its 110 data feeds per vehicle, Challenger 2 'Black night' with 100+ data feeds per platform and UAVs, FOBs and OPs, each will have an array of instruments, networked sensors and cameras. Today these data feeds come from ANPR, facial recognition, logistics tracking and direct from the soldier who can now carry an array of environmental/ health monitoring sensors. This also needs to integrate with data feeds from allies eg NATO, local forces and other partners. And there is also own pre-developed data repositories eg GEOINT, IMINT and theatre specific intelligence. But in today's Virtual War one of the largest data feeds that can be exploited is the tsunami of data from Twitter, Facebook, Instagram etc, required for real-world sentiment analysis and OPINT.

"We will focus on gaining 'Information Advantage' as the character of warfare changes. The effective collection, analysis and dissemination of vast qualities of data will enable us to understand how our adversaries are thinking, how they will act against us and how we can deter or defeat them" – MOD Jan 2019 [6].

At the same time, our adversaries have digitised their world, processing similar data feeds coming from their perspective of the same BattleSpace. As defined by our advisories in Systems Destruction Warfare doctrine [7], they are also trying to exploit, disrupt, confuse and make us doubt the data feeds in our modern Systems-of-Systems battlespace topology (Figure 2), as we do the same to them.

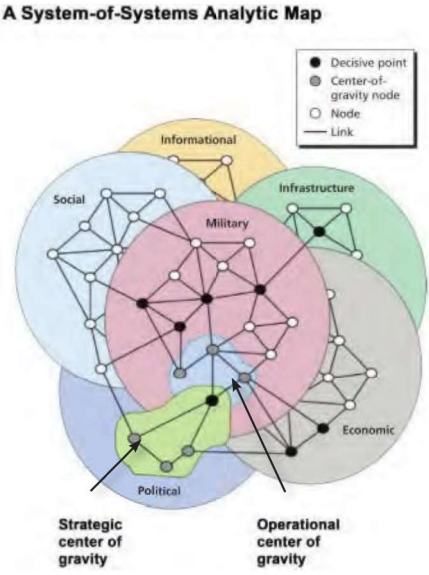


Figure 2 The Systems-of-Systems Topology of a modern battlespace [8].

Intelligentisation is the application and utilisation of all modern technologies to enable and support decision making. To fight at pace in the cyberspace domain, a 'Smart' army has to use advanced digital compute platforms that employ AI applications to process all this data held in a shared data-warehouse to evidence and improve battlefield decision-making. As the Master of Signals has directed, the Corps must *'deliver and manage agile digital data feeds and services across application, network and infrastructure platforms; protect our data feeds/information and at the same time exploit/disrupt our adversaries; and advise commanders on the use of all these data feeds and information capabilities'* [9].

To enable the delivery of this deployed compute fabric and at the pace, will require; a secure transmission fabric to transport any data on demand; federated multi-cloud, multi-tenanted hyper-converged compute platforms; and, the agile integration of applications using this infrastructure to store, analyse and visualise data in real-time.

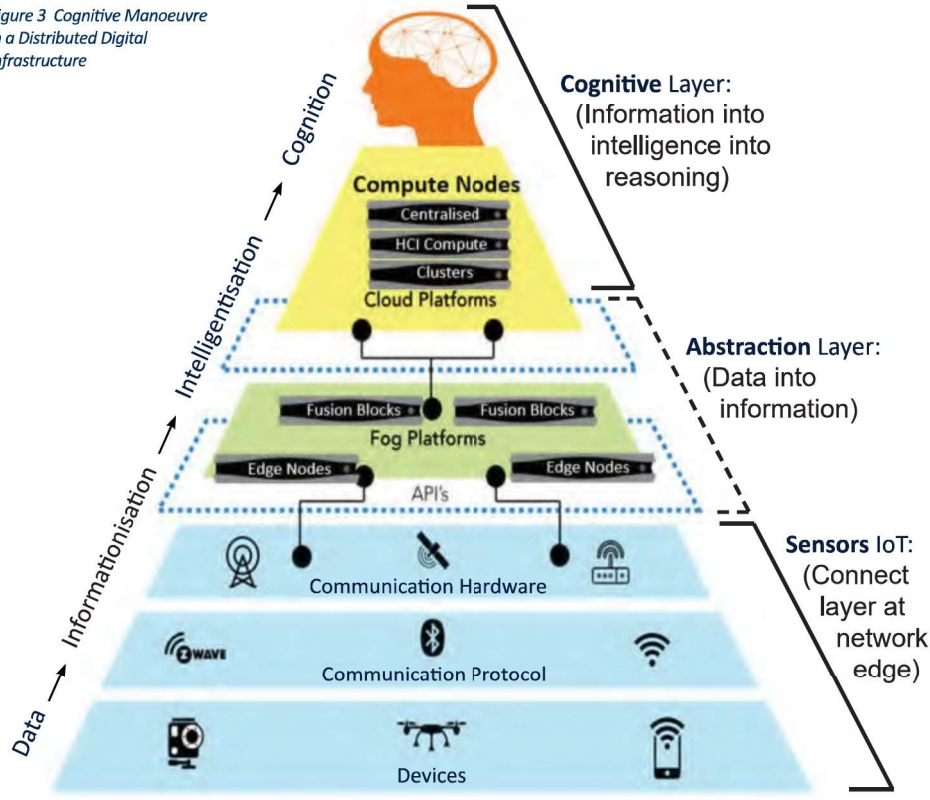
Cognitive Manoeuvre: It is now widely recognised that in the Virtual War speed will trump accuracy and speed will be the new measure of success. Thus, if a commander can just ask an AI web-bot like Alexa™ to search, analyse and deliver a live information product from the global data-sphere in nanoseconds, then the future value of military information services needs to be reimagined.

> *'Defence has a plethora of high-quality intelligence analysts but is it ready to exchange two-thirds of them for data scientists?'* [10]

The live processing of the torrent of OSINT/OPINT and integration with a myriad of other data feeds using AI algorithms in a Distributed Digital Infrastructure [11] is highly likely to be the primary role of the Corps in a Virtual War. To provide context, background and understanding in order to support better decision-making in the cognitive environment, in the context of a live, dynamic and confused battlespace, is also likely to be the role of Military Intelligence. Air Vice Marshall Johnny Stringer, JLF CoS summarised it recently *'...the need to understand and fuse this open-source intelligence with other feeds will place increasing demand on automation and big data analytics: without this, we risk generating even more 'Collect' of raw data without the means to 'Process & Disseminate' refined and timely intelligence product'* [12].

The intelligence analyst's role in the Virtual War will likely change to that of a story-teller of the actual reality devoid of nuance or ambiguity in a coherent manner that commanders understand and internalise. J2 operators will need to work closely with J6 platform operators to translate, interpret and fuse the data feeds into intelligence product, then articulate the aesthetics of what is happening all around the multi-dimensional, multi-domain battlespace including the implications on the commander's options. This understanding relies on the transport and fidelity of the data feeds into these AI algorithms and the correct visualisation of the analysis to deliver accurate intelligence output (Garbage in, Garbage out). To stay agile, relevant and dominant in the Virtual War, J2/J6 need to provide a sense-making cognitive service for commanders based on accurate data analytics but interpreted and contextualised by a human analyst. Human experience still cannot be automated nor delivered by a machine.

Figure 3 Cognitive Manoeuvre in a Distributed Digital Infrastructure



3. Virtual War CONOPS

The tactical playbook for warfighting has been constantly updated over millennia. Virtual war is no different: There are principles, concepts and tactics to be developed. As Deputy US Defence Secretary, Bob Work said: *"...for the millionth time, it is not about technology: It is about the integration of operational concepts and organisational constructs that will shape the way we integrate and use the technology."* [13] Below are some of the concepts that the Corps will need to develop, exercise and train.

3.1 Operating Principles

Integration: The focus on technology should not distract from its integration and fusion into military strategy. The winning advantage in a Virtual War will be the capability of the J6 planners to comprehend, visualise and integrate creative CIS solution platforms for CyberOps, InfoOps and SocialMediaOps into the battle plan. It also relies on the Information Warfare Officers' innovate application and synchronisation of these technologies with the Joint Ops teams to deliver a combined military effect across all the domains in the multi-domain battlespace.

Simultaneity: Contemporary technology is very capable of providing a military effect on its own but its greatest utility lies in delivering a synthesised joint effect across the domains. When Virtual War solutions are incorporated into a kinetic effect environment and applied cooperatively, simultaneously and synchronized, it will produce a concentration of effect exponentially greater in all the domains. Economy of effort can also be achieved by the judicious prosecution of limited offensive actions in cooperation with information/social media communication to deliver the maximum effect. Essential in controlling and coordinating the myriad of interconnected activities, will be the integration and adoption of a distributed multi-domain C5ISR Joint BattleSpace Management system.

Global Systems Engineering: Caution need to be given to proponents of cool new technology with unproven military application. Flashy new technologies will only useful if they are to enable a military capability or effect as part of a systems engineering solution. Suitably Qualified & Experienced Professional (SQEP) Royal Signals *Digital Engineers* will need to both grasp the military challenges of the commander and comprehend the contemporary global technology landscape so they can envision and deliver creative technical solutions to these unique military problems ... and at pace. Only by repeated exercising concepts, technologies and skills development in realistic military exercises will innovative integrated combat systems be shaped, tactics developed and new doctrine established.

Data Localisation: Storing data in the wrong location in a global system-of-systems will kill most applications due to latency in long reach back or reach forward links. Efficient operations of military CIS will require delivery of the right information, at the right time, to the right decision-maker (which could be another system). It is critical to be cognisant of where the data is located and the location of solutions used to transport, integrate and process it. By using contemporary Information Exchange Requirements (IER) processes and service-driven demand planning, decisions will need to be made by J6 planners on the technical solutions, location and transport media to enable it. The Corps' challenge will be to develop SQEP signallers and officers to deliver creative, innovative and bold solutions - globally.

Data Sovereignty: The precise location of data in a global System-of-Systems will also have significant legal implications in future wars. During a Virtual War, the military must still follow the law, whilst this is generally optional for our adversaries. Legislation like the General Data Protection Regulations (GDPR), global telecom regulations and country-specific cloud/data sovereignty laws will make fighting the Virtual War a legal minefield. "LawFare" could conceivable totally frustrate the actions of a careless CIS commander resulting in negative implications in the physical domains. Several states actively practice Lawfare as policy and have it established in their military doctrine during a Virtual War. Only by education, training and a thorough understanding of these topics will Corps commanders be enabled to observe, comply and advise on the commanders' obligations.

3.2 Computer Infrastructure & Networking

Virtual War has only now been made possible by the massive advances in technology infrastructures these past few years. Enterprise computing, networking technologies and application provision have changed so dramatically in the past 10 years that they bear little resemblance to our current battlefield CIS. Virtual war now requires a reimagination of how a Signals Corps (in conjunction with the Intelligence Corps) would deliver agile information services across these contemporary infrastructures, networks and battlefield ICT services.

Computing Power in warfare was first used during World War II to break Nazi codes and calculate artillery firing tables. Within a few generations military mainframes appeared, the Internet emerged and desktop PCs connected to centralised Army servers were the default military computing architecture. The physical size, electricity consumption and complexity of these servers meant that this computer infrastructure needed to be racked in a permanent data-centre building anchored firmly in a PJOB. During peacetime telecoms providers like BT provided networks to link these machines, but during war access to them required long (and expensive) reach-back satellite links. The complexity of these sprawling solutions also meant that only the geekiest computer scientist types were allowed to configure, programme and operate these machines. Other than administrating the deployed force in theatre, their utility to assist in the fighting of an expeditionary war was close to useless.

In the early 2000s specialist software called *Virtualisation* was used to Converge these Infrastructures. It linked all the separate computer chips, memory and disks to form logical Virtual Machines (VMs). In 2012 the concept

was perfected leading to *Hyper-Converged* Infrastructure (HCI) which totally re-architected, simplified and commoditised data-centres into boxes no bigger than a large briefcase. As the same time, revolutionary advances in the performance of computer chips, disk-storage and networking mean that today, a single HCI 'node' has enough computational power to easily run all the applications and services needed by a Battle Group HQ. With the inclusion of flash memory, Solid-State storage Drives (SSD), parallel addressable memory chips and fibre interconnect networking, these nodes can be integrated into 'blocks' to provide computers so powerful that could each run a small city. When these computer 'blocks' are stacked (*like Lego*) to form a 'cluster', they work as one homogenous computer to provide unimaginable compute power and storage capacity.

Today a virtual warfare commander can have virtually limitless compute power in his tent. The question now for the Corps and its J6 planners is to imagine how they can use this weapon to deliver battle-winning applications and services that enable the commander to dominate both the information and physical domains.

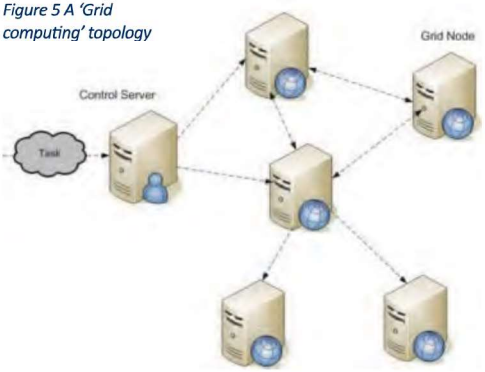
Network The future demand for imagery, OSINT data feeds and battlefield management systems that synchronise the unity of effort will require the transmission of 1000 times more data, 1000 times faster than current in-service systems. The virtual battlespace customer will expect EVERYTHING, EVERYWHERE, NOW.

New traffic bearers such as subsea cables, brown fibre, Free Space Optic (FSO) lasers, 5G and High-Altitude Pseudo-Satellite (HAPS) *see Figure 4*, are planning to transport data at these rates so in the near future an increasingly larger share of the military network traffic will be moving across them. Essential to controlling this is the Software-Defined Wide Area Networking (SD-WAN) logical control layer sitting above all these physical networks operated by SQEP Network Engineers. This provides a seamless mechanism for integration, routing and security across all these physical bearers to form a robust Global Wide Area Network (GWAN) using a myriad of both commercial and military solutions.

Empowered Edge computing is the practice of processing data on devices at the very edge of the network i.e. on the front-line of the battlefield. This is where most data is generated thus by empowering these edge devices, we negate the need to backhaul the data to be processed/ stored centrally. Instead, edge devices are now becoming 'intelligent' and need only send tiny data packets or trigger signals eg the target ID from AI enabled facial recognition camera device outside an OP. Modern edge networking architecture provides solutions to these challenges of bandwidth constraint, connectivity and latency. The use of thousands or millions of these devices (mostly sensors) is about to grow exponentially thus architecting and deploying a military Low-Power Wide-Area Network (LP-WAN) transmission architecture that forms a peer-to-peer Mobile Adhoc Network (MANET) at the front-line of the battlefield will require a new breed of SQEP military Network Engineers.

Distributed Digital Infrastructure (DDI) is the architectural term that describes all of the above when linked together to form one single system-of-systems. It is sometimes described as 'grid' computing (Figure 5) where various nodes (servers) are connected together by various network links. This Peer-to-Peer type network uses special control software embedded in each node to give the impression that each user has the whole network resources available (a pseudo-private version of the Internet).

Figure 5 A 'Grid computing' topology



Modern High Bandwidth, Low Latency communciations equipment

Figure 4 A High Altitude (80k ft), Long Endurance (1 year) UAV with Comms Payload

Future Battlefield Computing Infrastructure & Networking Topology

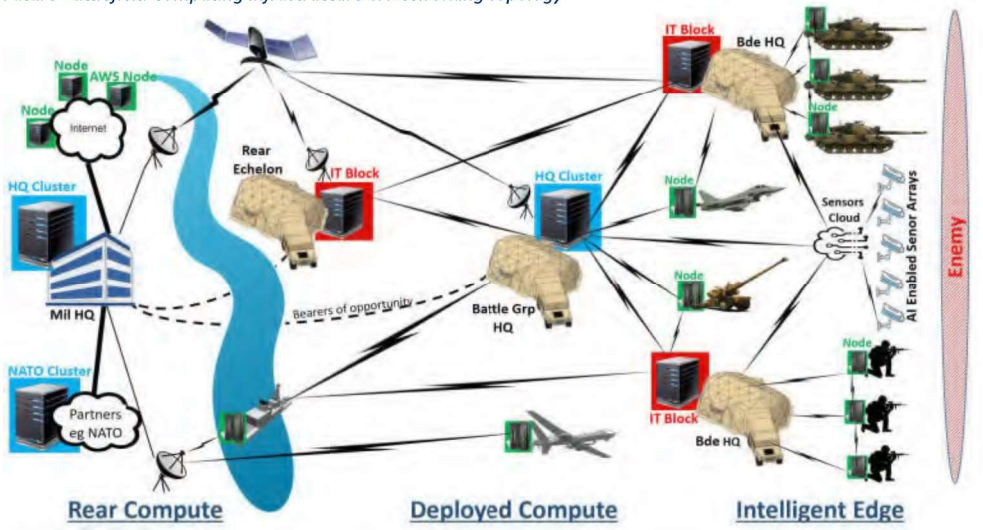


Figure 6 A Distributed Digital Infrastructure (DDI) topology

One of the advantages of this type of networks is it all works autonomously, automatically handling failures in a node, is self-healing if a fault occurs and instantaneously switches to backup nodes if the primary controller node is destroyed. The science was originally designed for a nuclear era military but then commercialized and hyper-scaled to deliver omnipotent services from Google, Facebook and Amazon. It is this architecture that underpins modern cloud services like Uber, Airbnb and Netflix.

When this cloud architecture is deployed in a virtual warfare scenario, it would enable J6 planners to push enterprise compute power out to all edges of the battlefield, unifying soldiers, devices and compute power into one single enabled force.

By leveraging other private clouds, scale-up classified solutions can be provided on partner cloud eg using NATO's Federated Mission Networking applications for planning or logistics. By leveraging other public clouds, scale-out unclassified solutions can be provided on public computers eg on AWS Cloud for Sentiment Analytics of OSINT. The re Defined Combat Network Radio services inside a secure cloud. Overall the benefits of using DDI (Figure 6) is that it will improve the end-user experience, provide stronger integration/service continuity across networks, reduce latency, allows geo-diversity and tighten data sovereign compliance.

The implications for defence are enormous. Because computing power is now virtually unlimited and the price so low, its use in virtual and contemporary warfare has to be totally re-imagined. With this power, we need to reimagine how we achieve military superiority in both the virtual and physical battlespaces, defend this architecture[14], and protect our data. At the same time, we need to imagine how we would disrupt and exploit our adversaries' data. We need to imagine how would we dominate this vital ground, similar to what our adversaries are already planning to do to us[7]. Failure to deploy, experiment, train and exercise manoeuvre with this Technology Stack (Figure 7) will leave us with an inability to advise the commander on the use of their information capabilities, leading to a failure of the commander to deliver physical and information superiority on the battlefield.~

3.3 Enabling Applications & Services

With the physical infrastructure established the Corps SQEP System Engineers can now orchestrate, configure and support the delivery of a range of applications and services to all users. Their role will be to virtualise, segment and share the physical environment amongst multiple tenants by virtualising the physical equipment into mission, theatre and operational domains. A myriad of software applications specific to the mission and each user can then be the provisioned on these open architecture platforms to process relevant data into information to be visualised in a meaningful way by their customers.

Platform virtualization or cloud orchestration software eg Microsoft Azure, VMware or Acropolis Hypervisors will allow Corps System Engineers to spin-up new platforms, domains and mission specific collections of virtual resources, and at pace (20 minutes). In these new virtual environments, engineers can install battlespace applications specific for each mission such as Microsoft products, Software Defined Radios (SDR), Geospatial data, C2 or C5ISR apps preloaded with specific GEOINT or IMINT content. But these platforms are also evergreen so will also host future as yet unwritten applications as well

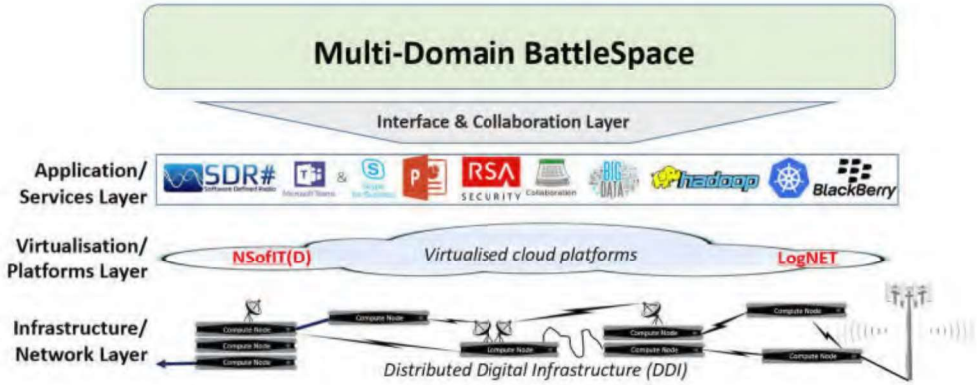


Figure 7 Technology Layers underpinning the Multi-Domain BattleSpace

as innovative applications such as private secure versions of Social Media platforms similar to Defence Connect. Much of this can be delivered on demand in the deployed HQ, then pushed forward into sub-HQs and to the edge of the battlefield to enable users to access the necessary data and toolsets required to fight their battle.

Big Data Analytics & Visualisation of vast quantities of data will be the crucial differentiator in a Virtual War. Analysing repositories of historical data and the fire-hose of live data feeds will give vital information but this needs real-time visualisation of this information in a format suitable to communication to commanders. Many databases, analytic and visualisation tools already exist eg heat-maps, trend prediction and scatter-graphs. However, the importance of having SQEP Application Engineers suitable trained, knowledgeable and exercised in their deployment, application and usage is required.

Machine learning & Artificial intelligence is *destined to fundamentally reshape defence*[15]. As an enabling technology it is fated to have the biggest implication on future war, but the compute and networking technologies mentioned above are the required hardware, network and application platforms required to enable it. Similar to training a voice-recognition tool, these software tools need to ingest vast qualities of historic data or experiences to train the application to recognised patterns and thus develop *intelligence*. This intelligence can then be used to dynamically predict future behaviours based on these learnt patterns. Military utility could involve pattern-of-life data analysis eg meta-data patterns from CCTV feeds could alert to irregular behaviours (eg US DoD Project Maven), visual activity triggers in video feeds, voice recognition of signals intercepts or decision support eg preventative/planned maintenance based on equipment usage, dynamic translation of languages and operational deployment decision support based on biometric IoT sensors worn by soldiers. The more data that is ingested, the more accurate and useful the AI systems will become.

3.4 Cognitive Effects

Weaponizing of Data in war requires totally new operational practices and tactics that leverage new business, technology and operating models to disrupt adversaries, exploit data feeds and augment/automate decision making (using AI) to deliver information advantage payloads. This provides commanders with a range of non-lethal effects, short of lethality. Control of a Virtual War will rely on parsing the torrents of sometimes conflicting and low-grade data feeds in conjunction with J2, into information and actionable insights for the commander … in real time. *'It will require both the agile exploitation of information as well as the ability to transmit one's message to the effect the behaviour of others'*. Deploying suitable erroneous data/false news into/around an enemy OODA loop, stealth technologies and cloaking/masking technologies is a practice described 1000s of years ago by Sun Tzu. Today the practice is widely used in social media and is systematically directed at soldiers/ leaders on the front line. As we attempt to deploy these weapons on our enemy, we also must be cognizant that we also need to defend against an enemy that will actively be doing it to us and our soldiers.

Assisted Decision Making is one of the key applications of all these technologies. As compute power and technology platforms begin to come on-line, cognitive systems engineering capabilities using AI will be increasing move data up the cognitive hierarchy, from being just descriptive of what is happening (Big Data & Visualisation), to becoming more intelligent (decision support).

Using a counter-insurgency example, cognitive decision-support systems engineering could provide the following outcomes. By using AI technologies better decisions could also be made and in real time if necessary. The main five outcomes could be;

Analytics v Human Input - Decision Support Model

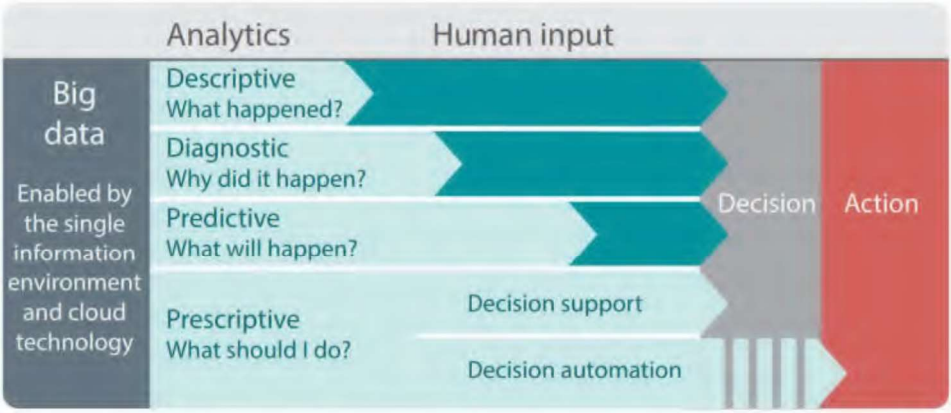


Figure 8 Types of analytical/decision support (JDN2/17)

- **Descriptive** - *4 known militants in a group of 30 men have been detected by camera 1 and 2;*

- **Diagnostic** - *3 are members of a faction said they would attack a military target on Facebook.*

- **Predictive** - *they are heading East from camera 2 loc, at 4mph, 2miles from the A Coy position.*

- **Prescriptive** - *recommend alerting A Coy guard, QRF and air support.*

- **Automation** - *triggered the alarm at A Coy, messaged QRF with the attack time, messaged Air support.*

'Military supremacy won't be achieved through the interplay of advanced capabilities alone; it will be achieved through the ability to capture and synthesise content to make better decisions, faster than an adversary.'

Adam Misiewicz, Intelligence & National Security ANZ at Accenture[16].

Analytics v Human Input - Decision Support Model

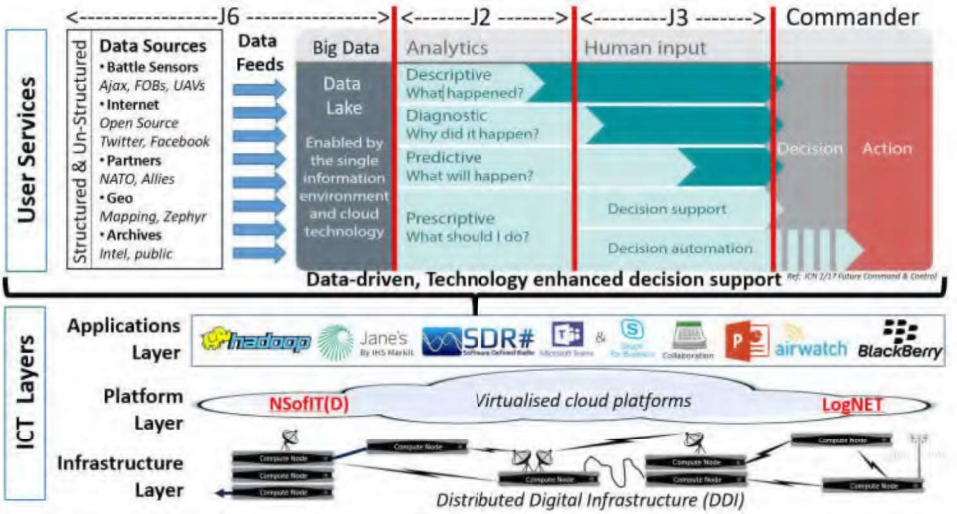


Figure 9 ICT enablement of the military decision support systems (JDN2/17)

3.5 Cyber Security

As the CEMA threat evolves so too must an organisation's holistic security posture to deal with these dangers. It is perceived wisdom by the ICT community that a cyber war would be fought over control of infrastructure eg networks, devices or control systems. But as social platforms and networks have grown, cyber influence weapons for precision targeting and control of the citizen are a more preferred weapon for adversaries. Autonomous web-bots, Russian *sock-puppets*, polymorphic code and message amplification tools that target the minds of citizens easily, cheaply and with zero causalities, these are the main cyber weapons in Virtual War. Whether the political objective is regime change, counter-narrative, or a prelim to a physical invasion, information warfare is a far more alluring lever of power to a modern-day politician than troublesome kinetic engagements. Hardening architectures, systems and capabilities are essential, but more important is agile, adaptive and mobile SQEP Cyber Engineers that learn attacker tactics, build threat intelligence and use AI enabled defensive and offensive weapons against them. We need a Cyber capability that automatically detects vulnerabilities and attacks. It if is our soldiers versus their computers then we have lost this war. It's got to be our computers against their computers.

4. Talent & Leadership

Commanders, staff and force elements will need to be organised, equipped, trained and exercised to operate and manoeuvre in a Virtual War.

Talent Gap: The future Signalling and Intelligence skills required to deliver the capability above will need new non-traditional skills with a balance of both generic ICT expertise and specialist product/ service-based engineering. They will also need a mix of business knowledge, sector experience and contemporary soft skills, especially personal communications. Also, noticeable will be *'the balance between generalist and specialists will be increasingly tipped towards specialist career streams'*[17]. When this is all in place, repeated opportunities must be provided to integrate these diverse peoples during live military exercises into teams-of-teams. This will deliver fresh new thinking, new processes, procedures and information age doctrine as well as a CONOPS for their inclusion and utilisation in the overall battle plan.

The new Armed Forces (Flexible Working) Act is also a big step forward in maintaining specialist Regular skills and maintaining Reserve Forces as a key part of national flexibility and resilience. But there may be opportunities to be more creative in attracting and retaining increasingly high-end technology SMEs by providing unique Reserve opportunities and innovative engagement contracts. Further insight & skills could perhaps also be gained through working closely with modern technology businesses to ensure a pipeline of contemporary knowledge is more readily available, though there would need to be clear advantages for the companies as well. These talent gaps are at their most acute in the fields of Architecture, AI, Analytics, Cyber-Security as well as product knowledge of all new technologies.

Civil/Military Leadership: Alongside the transformation to this new character of warfare, also approaching is a new era for military/civil fusion. To realise the full potential of the opportunities in the Virtual War, the development of the operational control of these technologies will require a more hybrid whole-government, military/civil C2 structure. The scale of the shift required and the leadership challenge involved is perhaps not currently as well recognised or defined as it could be.

> *'These technologies will fundamentally reshape the character of war, if not - as some have speculated - its very nature'* [18].

Digital Officership: In Virtual Warfare technical and tactical competence alone will no longer be sufficient to enable leaders to command. To exploit the speed advantages offered by modern technologies, junior military personnel must be enabled and empowered to innovate, develop and deploy these innovative tools, devices and Information Age practices. The military has a long history and tradition of innovation and in the words of Steve Jobs 'Innovation is what distinguishes leaders from followers'. With the new character of warfare, the most effective leaders will be those comfortable leading in this complexity and ambiguity, amid the chaos of a virtual battlespace and training must reflect this. Maximum effect in the virtual domain will come from the application of information reach, manoeuvre, tempo and fires as it would in the physical domain, as part of the combined effort. Becoming even more agile, nimble, adaptable and flexible in addressing complex, sticky and wicked socio-military problems will require different – even radical – thinking. The development of a dynamic information age culture in which innovation, enterprise and agility (in all domains) is encouraged and valued, will require the shedding of any remaining vestiges of an industrial age culture based on rigid doctrine and hierarchy. In an ever increasing complex, multi-faceted and unpredictable battlespace, the future threat environment will require leaders to be equally competent in inspiring, enthusing and energising their soldiers, as they are at delivering technological effects in support of their commanders intent.

Potentially great benefits for leaders could come from a very close relationship with the UK technology industry, suppliers and general commercial businesses. Attendance at supplier seminars, trade expos, university lectures and embedding with suppliers are a few simple ways this could happen. There is further potential to accelerate the gains of fighting in the virtual domain through embedding personnel from technology suppliers, university researchers and creative thinkers into the Corps military exercises. Through better understanding, they can challenge and create solutions to satisfy the demands of modern warfare.

If the Corps is to deliver the solutions, a radical re-imagination of the technical capabilities needed and the technical competencies required of our soldiers and officers is essential. In the next war the Corps CIS Planners, Information Warfare Officers, Data Analysts, Cybersecurity, Networking & IT Support soldiers[19] will need to be as competent at winning the cyber, information and intelligence campaign as they are at the military campaign. Virtual war will more than ever rely on bright, articulate and innovative young Digital Engineers lead by intelligent, dynamic and professional officers with an infectious energy to succeed.

5. Conclusion

There has been a paradigm shift in the nature of armed conflict in the past 10 years. When combined with the transformative effects of new digital technologies and social media on society, predictions are challenging even the most futuristic defence planners. The response to this seismic shift needs to be bold, radical and visionary. It will require fundamental new thinking, a challenge to traditional comfort zones and a fundamental shake-up of entrenched industrial age military culture. It will also require our bureaucratic purchasing processes to be overhauled to instead be driven by the agile facilitation of new information age multi-domain fusion doctrine, at pace. It needs military decision making enabled by contemporary technology solutions and military procurement based on commercial business services, outputs and performance.

Whilst many see technology as the panacea to solve all issues in defence, many historic innovations have failed to live up to their promise. But equally so, strategic dithering on new technological solutions will also prove fatal: We have all already been mobilised as combatants into a lukewarm virtual war played out daily in our social forums and online media. In the same way that Netflix, Uber, Airbnb etc have quickly risen to dominate their operating domains, the military that transforms, innovates and upskills its people to dominate in the cyberspace domain will win the territorial battle in Virtual War.

6. Next Steps

Defence Secretary Gavin Williamson in Jan 2019 stated that *'The international security context has become darker and more dangerous' and he 'will now be investing in a range of new 'Spearhead' innovation programmes to apply cutting-edge technologies to contemporary challenges ... delivered through a new £160m Defence Transformation Fund ... and a further £340 million as new ideas are generated ... to drive innovation and transformation of military capability'*[20].

General Sir Nicholas Carter, Chief of the Defence Staff, in June 2018 stated that he now requires the same effect delivered by a Strike Bde of 3000 soldiers, as would have been delivered by a division of 15,000 soldiers[21]. The ability to use information as a force multiplier across the Army's Single Information Environment (SIE) must be considered the ultimate key enabler of this vision. To deliver this, both industry and the Corps have to understand and mobilise these capabilities now to fight this war. The future weapons, tactics and doctrine are yet to be conceived, developed and delivered, but doing so as we contest the next war is too late. In conjunction with British industry, setting military challenges that need visionary conceptual and creative solutions will drive military innovation, develop new industry products and deliver international business advantages post Brexit. Now is the time for risks to be taken, to be bold, to experiment with novel technology applications and rapid prototyping based on the understanding that failing fast, safe and at relatively low cost is a success in its own right. The Corps needs to exercise new technology solutions in combat like scenarios to deliver new military tactics, experiences and doctrine.

Those that are to prevail in the next war will not be those with the best weapons or latest technologies, but the digitally savvy Corps that have learnt to best adapt, integrate and employ current contemporary technology to deliver military effect.

Capt Martin Crilly is a Reservist with 39 Signal Regiment. He is the Chief Architect & Engineering Authority to BAE Systems in the Middle East. His background is in contemprary ICT architecture, strategy, cyber-security, J2 and J6 with previous military roles/ops in BFC, ISS Ops Plans, GOSCC, DE&S Maritime and others. For more information and articles on Virtual War and similar topics, 'follow' him on Defence Connect.

References

[1] *MOD, (2014) Future Operating Environment 2035 9*
[2] *Carter, General Nick (2018) Annual Chief of Defence Staff Lecture Jan 2018)*
[3] *The Changing Character of Future Warfare [video] Available at https://www.youtube.com/watch?v=0VsikOe_-wg [Accessed 21 Apr 19].*
[4] *Joint Concept Note 2/17, Future of Command and Control*
[5] *SFIA version 7: https://www.sfia-online.org/en*
[6] *Mobilising, Modernising & Transforming Defence Programme Report (Jan 2019)*
[7] *Engstrom, Jeffrey (2018) "Systems Confrontation and Systems Destruction Warfare, How the Chinese People's Liberation Army Seeks to Wage Modern Warfare", RAND 2018*
[8] *US Joint Chiefs of Staff, 2011a, p. Figure IV-2*
[9] *Pope, Lt Gen N.A.W (2018), Master of Signals Intent for the future*
[10] *Rigby, Jon (ex Director of Cyber, Intelligence and Information Integration (DCI3)) & Rob Jones (ex Army HQ) & Ross Baily (ex RAF Intelligence) (2018), A question 4 moment - A perspective on changes to the challenges and imperatives within the SIE, Leidos 2018*
[11] *https://www.computer.org/publications/tech-news/data-center-insider/how-to-manage-todays-hybrid-it-infrastructure*
[12] *Stringer, Johnny Air-Vice Marshal (2018) Change Character, Changing Context, Enhancing Airpower employment in the RAF 2nd Century, RUSI Journal 163:3, p34-42*
[13] *Work, Bob, US Deputy Secretary of Defence, Washington, Remarks to the Association of the U.S. Army Annual Convention (2016)*
[14] *Defendable Architectures: Achieving Cyber Security by designing intelligence driven defence, Lockheed Martin Corp (2019)*
[15] *https://www.defenseone.com/ideas/2018/05/ai-begins-reshape-defense-heres-how-europe-can-keep/148318/*
[16] *https://www.linkedin.com/pulse/new-art-war-ai-changes-game-adam-misiewicz/ (2019)*
[17] *Boyle Report (2016) into future of Royal Signals*
[18] *Brooks, Risa. (2018) War on the Rocks: Technology and future war will test US civil-military relations*
[19] *Crilly, Capt Martin (2016) "Today's Battlefield", RSI Journal Summer 2016, p21-24*
[20] *Mobilising, Modernising & Transforming Defence Programme Report (Jan 2019)*
[21] *Defence Vehicle Dynamics (DVD) (2018). [video] https://www.youtube.com/watch?v=HdAeb7F9OXE [Accessed 21 Apr 19].*