DEFENSE AND INTELLIGENCE

The urgent need for hyperscale cloud now!

Lloyd Hewitt, Robert Alders

The Case for Hyperscale Cloud NOW!

Maintenance of the post-war global order is entering a heightened phase of competition with adversaries increasingly looking to exploit the surge in technological advancements to get ahead. There is an urgent need for defense organizations to develop and adopt emerging and disruptive technologies that will support the maintenance of a dominant position. However, the race for 'digital advantage' can't be won through reliance on current siloed and technologically constrained Information and Communication Technology (ICT) environments that predominate in defense and intelligence organizations – the answer to this dilemma is through increased adoption of hyperscale cloud. This paper provides insights on why this is the case.

Background

Over recent decades, Defense and Intelligence organizations have seen unparalleled and constant change, as they respond to the emergence of a new and transforming world. The rapid and disruptive advancements of technology, particularly accelerated by the global pandemic, is a leading force of change. However, when considering the digital transformation of Defense organizations, it's crucial to examine it within the context of evolving geopolitical dynamics and the changing nature of warfare. This includes assessing the impact across global threats, regional instability, emergency response, hybrid warfare, and cyberattacks aimed at disrupting both military and industrial infrastructure.

Defense and Intelligence organizations must continue to adapt to this increasingly complex landscape. Addressing these challenges will require these organizations to compete continuously across all domains, adopting better, smarter, and more flexible operations that are integrated and imbued with agility to over-match adversaries. The adoption, continuous innovation, and democratization of technology will be key to enabling this response. Moreover, this adoption encourages a growing reliance on sharing data across a secure, singular, resilient, and adaptive digital continuum, and exploiting that data through contemporary developments will enhance human/machine teaming.

Furthermore, the growth in Internet of Things (IoT) capabilities is driving maturity in sensors, data gathering, analysis, and visualization, all of which can be delivered at the tactical edge for deployed forces. Artificial intelligence, cloud computing capability, and sophisticated simulation techniques are being fused with new and evolving communications technologies, such as 5G and space-based capabilities, which together have the potential to revolutionize mission planning, rehearsal, and execution.

In recent times, the onset of a global pandemic was a catalyst for Defense organizations to reconsider their ICT posture and rapidly mature their capabilities. The need for sustained remote working necessitated the use of commercially available web conferencing and collaboration tools, which ultimately drive **modernization of the workplace**. Further, forward-thinking Defense organizations embraced this transformation opportunity to enhance their digital engineering, introducing defense software factories and contemporary methodologies to build systems with greater effect.

Background *continued*

The progress in technological advancement has led to an increased need for **trusted and secure infrastructure and services.** Defense forces are actively seeking ways to enhance the rapid and secure scalability of their environments to effectively address emerging demands.

By leveraging a variety of modern technological capabilities and embracing the growing utilization of agile and scalable computing resources, militaries are enhancing their capacity to leverage data. This improvement contributes to heightened mission capability, readiness, availability, and interoperability throughout the entire spectrum of defense missions. It also reduces security vulnerabilities, and scale to the reliable and modern infrastructure required to **optimize operations and enhance data-driven decisions.** Furthermore, Defense organizations are embracing **zero trust architectures** and modern security operating frameworks to **protect their information domain and grow their cyber force capabilities,** ensuring that the gains they make in information maturity are adequately protected and securely shared.

That said, even as we have witnessed this increasing need to transform, we still see a slow adoption from some organizations to fully embrace the power of hyperscale cloud. Political drivers, designed to build and maintain local industry content are also considerations that give pause to thoughts of exploiting the global reach and market-leading capabilities seen in hyperscale environments. It is time to clearly state why the use of hyperscale for Defense and Intelligence organizations is no longer a 'nice to have' but rather a necessity to stay at the forefront of the race for emerging and disruptive technologies that will underpin military capability into the future.

Achieving Digital Advantage

As we have seen throughout history, a key element in determining the outcome of global conflict is the application of industrial power, notably where allies were able to mobilize their economies and produce vast quantities of weapons, equipment, and supplies that engendered a material advantage over their adversaries. During the Cold War, an irrefutable technological advantage was held by the US and its allies. Their industrial power was able to foster a culture of innovation and entrepreneurship that stimulated scientific and technological breakthroughs, which was shared across the allied partnership for advantage. Contemporary thinking also highlights the importance of technology in global power competition. Christian Brose, in his acclaimed book[1], argues that the US military must "leverage artificial intelligence, autonomous and smaller systems, cloud computing, and other emerging technologies" to effectively close the sensor to effector loop.

Given the increasing race for technological advantage, allied nations must therefore consider how they can increase their tech intensity[2], to provide 'digital advantage' over their competition, where 'digital advantage' is understood to be a force holding the initiative in terms of their ability to develop and deploy digital capabilities to enhance their strategic, operational and tactical objectives. Many forces include 'information advantage' into doctrine as one of the Joint functions[3] but we see 'digital advantage' as going beyond information. Digital advantage is centered on winning the race to achieve 'tech intensity' as well as developing a digital philosophy at the core of the Defense and Intelligence organization's processes, products, and services, including its decision-making and communication capabilities. We also consider that digital advantage needs to be enabled by fostering an environment and culture that emphasizes the importance of creating a supportive and conducive context for digital transformation and innovation.

For Defense and Intelligence organizations, achieving a 'digital advantage' is crucial. It not only establishes the foundation for ensuring information superiority during missions but also accelerates the design, construction, and transition of novel capabilities into service. This expedites the capability lifecycle and incorporates simulation technologies to optimize force generation activities.

Achieving Digital Advantage *continued*

In November 2022, the Science and Technology Committee of NATO released its report on Technological Innovation for Future Warfare[4], the report noted that “Emerging and Disruptive Technologies (EDTs) are expected to play a crucial role in developing NATO’s military capabilities” and defined eight “major strategic disruptors” relevant to NATO’s capabilities between 2020 and 2040, which were: data; artificial intelligence; autonomy; quantum technology; space technologies; hypersonics; biotechnology and human enhancement (BHE), and; novel materials and manufacturing (NMM).

In April 2023, the Center for Strategic & International Studies produced its report ‘Seven Critical Technologies for Winning the Next War’[5] The seven technologies of the title were defined as: Secure and Redundant Communications; Quantum Technology; Bioengineering; Space-Based technology; High Performance Batteries; AI/ML; and Robotics.

Furthermore, according to the NATO Chief Scientist, Dr Bryan Wells, future military capabilities will increasingly depend on:[4]

Intelligent technologies which will exploit AI and new analytic capabilities.

Interconnected technologies which will exploit virtual and physical domains.

Distributed technologies which will employ decentralised and large-scale sensing, storage, and computation.

Digital technologies which will blend human, physical, and information domains

Five imperatives for hyperscale adoption by Defense

There is, of course, close alignment across the technologies listed in these reports but what is probably more important for the authorities that are invested in realizing these technologies (both industry and defense), and doubly so for the dependencies highlighted by Dr. Wells, are the capability gains that can be achieved by delivering these emerging and disruptive technologies. The race for 'digital advantage' can't be delivered from current siloed and technologically constrained ICT environments that predominate in defense and intelligence organizations – the answer to this dilemma is through increased adoption of hyperscale cloud, but why?

Innovation and speed to value

First and foremost, innovation and speed to value. Retired Vice Admiral Ann E. Rondeau offers an inside look into how defense organizations can adopt digital tools and adapt with emerging technology. She says, *"Command and control is essential for decision-making in the end, that has to include some combination of AI, machine learning, and all the other adaptations technologically, alongside in parallel with an exquisite timing with a human ability, and the human value of making decisions in that cycle. So, I think that the digital world has changed command and control, but the objective of that is to make really good decisions."*
– Retired Vice Admiral Ann E. Rondeau[6]

We have already highlighted the importance of industrial power in near-peer competition, as well as the example of technological superiority that finally won the Cold War. Staying at the forefront of the technology and innovation curve is critical and we are seeing this play out in the race for AI and quantum. But leading the charge, is dependent on high performance compute and heavy reliance on the latest chips that can only realistically be consistently updated and accessed via hyperscale capabilities. Defense organizations are rapidly recognizing that on-premise or even managed service providers (in so called private clouds) cannot realistically compete with the exponential growth of hardware resources that are available at hyperscale.

It is not merely the innovation cycle that requires acceleration. There is also the need to quickly and effectively deploy new digital capabilities to the theatre of operations and tactical edge, be it updating sensor capabilities on the latest aircraft, or providing an urgent security patch to a forward operating base.

Five imperatives for hyperscale adoption by Defense *continued*

Effective Mission Planning Operations, based on DevSecOps principles, is a vital element of a software intensive battlespace. Microsoft capabilities are utilized globally in advanced mission system design and development, such as seen in the United States Military Platform One[7] for systems design and deployment to Azure Government Classified Clouds. Here and elsewhere, Microsoft provides enterprise cloud capability in Azure on classified workloads and infrastructure that support all aspects of mission system design, development, and deployment to meet this need.

Connectivity and interoperability

Next is connectivity and interoperability, including integration of joint and coalition forces. Military organizations require disparate forces and their force elements to be able to collaborate seamlessly, wherever they may be across the globe, and with an ability to consistently breach the divide between headquarters and the tactical edge. This type of collaborative environment should also be available for industry partners and government and non-government agencies when required. Provision of modern work tools and a continuum that is able to manage data flows from hyperscale to edge is core to this need.

Microsoft Azure is effectively a Global Computer, encompassing a world-wide network of data centers, servers, and networks that power Azure's cloud services. This network, distributed across multiple geographic regions, and via proprietary fiber and space-based communications, forms the backbone of Azure's infrastructure. It enables users to deploy and manage applications globally with low-latency access to data and services, providing the ideal platform for global connectivity and interoperability across disparate forces.

> "Tomorrow's fight will depend heavily on communications. Jointness of forces, operations with allies, and even tactical coordination between dispersed units depend on secure and ever-present communications."[5]

Five imperatives for hyperscale adoption by Defense *continued*

Security

Certainly, at the heart of the opposition that we see from Defense and Intelligence organizations for the use of hyperscale environments is security and the perceived threat to sensitive military data.

Dr. Marcus Thompson, retired Major General and former Head of Information Warfare for the Australian Defense Force shares best practices for protecting sensitive data and making risk-based decisions. He says, *"When there's a new piece of malware on the streets, every seven to twelve seconds, you know, you might be compliant, at that nanosecond, in that instant, you might be compliant, but a moment later, you're now being noncompliant."*[8]

We have consistently heard the argument that 'air-gapped' capabilities provide the best form of defense for the military. However, air-gapped environments are becoming increasingly more vulnerable to attack, with an increase in the insider threat from air-gapped systems. "In April and May this year, Microsoft observed a spike in activity against Western organizations, at which time roughly 46 percent of observed network intrusions were directed against organizations within NATO member states, particularly the United States, United Kingdom, and Poland."[9] Furthermore, network security is based on the connectivity of the system, rarely do private clouds (unless they are enterprise scale) have comparable network security systems, tools and monitoring that are available in a hyperscale Security Operations Center (SOC), and even at enterprise scale, so-called private cloud is significantly poorer in SOC performance to hyperscale cloud.

"Air gaps are no longer enough to protect networks from malicious attacks, as attackers can use various methods to gain access. therefore, organizations must extend their monitoring and inventory discovery beyond air-gapped networks to ensure their networks are secure and up to date with the latest technologies and security protocols."[9]

Five imperatives for hyperscale adoption by Defense *continued*

In the last 12 months, we have seen several high-profile insider attacks on government networks being made public, and evidence suggests that nation-state attackers have infiltrated and remained undetected in military air-gapped environments for extended periods. Furthermore, the attack-plane is increasing, as organizations look to exploit more IoT devices – "of the 78% of IoT devices with known vulnerabilities on customer networks, 46% cannot be patched".[9] The threat of AI poses an ever-increasing challenge as more nation state cyber-attacks move to AI-centric operations, requiring in turn more advanced AI defense. For example, China has around 15,000 cyber offence staff conducting cyber offensive operations. There has been a litany of attacks from the last 12 months that have targeted military organizations, as well as evidence that demonstrates that countering these types of threats requires the power and sophistication of AI computers, as well as access to the scale of data only seen at hyperscale.

Microsoft has one of the largest AI supercomputers in the world, just to handle threats! The power of this capability is extraordinary and currently handles 750 million security signals per second using AI. Furthermore, this capability ensures that Microsoft is able to provide access to real-time threat analysis enabling AI-driven defenses to provide rapid response capabilities to emerging cyber threats; far in excess of the speed of response for private networks.

Computational power

Another significant driver for defense's adoption of hyperscale is the availability of unconstrained access to computational power that is needed for the intensive collection, fusion and analysis of data, allowing commanders to make informed decisions in real time. Be it for simulations on complex, multi-faceted issues, such as force structure, digital engineering for new capabilities and assets, or the derivation of a commander's course of action the computational needs are immense and far exceed those realistically available on premise. This has been highlighted by the recent clamor from Defense & Intelligence organizations, for use of Large Language Models, to drive their modernization needs but, which themselves drive resource-heavy compute. Defense organizations cannot hope to maintain their 'digital advantage' through traditional means, instead they must embrace hyperscale, which can meet

Five imperatives for hyperscale adoption by Defense *continued*

an organization's growing data demands and add extra resources to large, distributed computing networks without requiring additional cooling, electrical power, physical space, or the extended time and elevated cost of provision on-premise. Furthermore, Microsoft Azure provides the compute, storage, and virtualization layers of infrastructure in a single-solution architecture, ideally suited for the demands of defense.[10]

Reliability and resilience

When considering reliability and resilience there is much literature that will point to how the hyperscale cloud is designed, bottom up, to provide high-resiliency and data replication through regional pairing, distributed regions and availability zones etc. Indeed, Microsoft Azure is the first hyperscale cloud provider to be certified under ISO-22301, demonstrating the ability to prevent, mitigate, respond to, and recover from incidents. However, for defense organizations, consideration of reliability and resilience must also include the potential for kinetic, as well as cyber-attack, in peace time and in conflict.

> "Defense against a military invasion now requires for most countries the ability to disburse and distribute digital operations and data assets across borders and into other countries."[8]

Five imperatives for hyperscale adoption by Defense *continued*

Resilience to cyberattack is covered above but it is worth noting that hyperscale cyber protection extends across the various spheres of attack, typical in transition to war, including cyberattack within the given geographic region, network penetration outside of that region, which may include espionage activities against allied nations, and influence operations targeting people globally. Defense against all these forms of digital attacks, requires a collective approach, across allies, partners and external agencies, which cannot realistically be achieved through the current fragmented cybersecurity landscape – and it is here that hyperscale cloud provides the gold standard for collective protection.

Furthermore, resilience goes beyond cyber defense. We have also witnessed, in the lessons identified from Ukraine, that early kinetic attacks included a cruise missile assault on a government data center and the innate vulnerability of local 'on premise' servers from conventional weapons. Here dispersal of the digital assets and infrastructure to the cloud has been a marked success, providing an obvious strategy for others facing similar threats. Providing a safe haven in the cloud for a nation's data (including critical infrastructure, supply chains and the administration of government), in the time of conflict, provides a level of resiliency during kinetic attack, that is not otherwise available. Consider the impact on the smooth running of a nation, if the data hosted in an on-premise capability is lost or compromised. Furthermore, the continuum to edge can still be maintained with mission essential data and algorithms available in hyperscale and the agility of mobile C2 serviced through connectivity, delivering containerized services when and where required, as dictated by mission posture.

The Final Word

To maintain digital advantage, defense organizations are reliant on the global defense industrial base. However, this can't be done by industry alone. General Bob Brown touches on the need for advanced technology to make quick, informed decisions, and the significance of collaboration with allies and partners. He says, *"It takes all domains, air, land, sea, cyber and space, effectively working together. I don't see how you can do that without the hyperscale cloud."*[11]

Defense also needs to come to the table with a desire to unburden its procurement constraints, which will aid greater innovation, and to take on the task of vigorously reviewing its policy direction and its place (or not) in a modern digital world, which can often stifle progress. At the crux of the ability to achieve the latter, is the need to understand and assess the risks versus benefits that greater adoption of hyperscale brings; we are keen to engage in this conversation with partners and customers alike. To ensure that we build the digital future for defense and the defense industrial base on a shared understanding and acceptance of the 'gives and gets'.

To learn more about how Microsoft's Defense and Intelligence team can help in your transition to hyperscale cloud, contact your Microsoft sales representative or technology partner today.

To hear more from defense leaders listen to the full episodes where they share their perspective on the value of digital transformation to support the defense continuum: 1) Modern Military Insights from General Bob Brown, 2) Technology Trends with retired Vice Admiral Ann E. Rondeau, and 3) Military Lessons on Cyberdefense with retired Major General Dr. Marcus Thompson.

[1] The Kill Chain - Defending America in the Future of High-Tech Warfare. Christian Brose, Hachette Books, New York, March 2022.

[2] Tech Intensity=Rate of Tech Adoption + Tech Capability. The rate of tech adoption refers to how quickly an organization can adopt the latest technologies, such as cloud computing, AI etc. The tech capability refers to how well an organization can innovate and build its own digital solutions.

[3] Joint Functions are related capabilities and activities grouped together to assist Commanders in the direction of Joint Operations: Command and control (C2), Information, Intelligence, Fires, Movement and manoeuvre, Protection and Sustainment (US Joint Publication 3.0 – Joint Operations)

[4] NATO Parliamentary Assembly, Science and Technology Committee (STC) Sub-Committee on Technology Trends and Security (STCTTS) Report, TECHNOLOGICAL INNOVATION FOR FUTURE WARFARE dated 20 November 2022 (2022 STCTTS REPORT – FUTURE OF WARFARE (nato-pa.int))

[5] 230418_Harding_Seven_Technologies.pdf

[6] Microsoft. "Technology Trends and Decision Advantage in Defense" URL: https://wwps.microsoft.com/episodes/tech-trends-defense

[7] Platform One. (n.d.). https://p1.dso.mil/

[8] Microsoft. "Military Lessons on Cyberdefense" URL: https://wwps.microsoft.com/episodes/military-lessons-cyberdefense

[9] Microsoft Threat Intelligence, Microsoft Digital Defense Report, Building and improving cyber resilience, October 2023.

[10] Microsoft. "Defending Ukraine: Early Lessons from the Cyber War."OntheIssues, (June 2022)

[11] Microsoft. "Digital Transformation in Modern Military Operations" URL: https://wwps.microsoft.com/episodes/modern-military-operations

Authors

Lloyd Hewitt

Hewitt, as an experienced business leader, and former United Kingdom and Australian Defense - Naval officer has worked in both public and private sector industries. As Director, Worldwide Public Sector, he is responsible for Microsoft's Defense Strategy where he relies on years of experience and intuitional knowledge of defense procedures and ecosystem. He is a vocal advocate for the adoption of cloud-based technologies to future defense missions.

Robert Alders

Alders has almost 30 years of experience in business consultancy, (ad interim) management and organizational change in both private and public sector organizations. As an Industry Advisor he works closely together with Microsoft account teams and their Defense & Intelligence customers in Europe on the successful adoption of cloud-based technologies, thereby exercising a 'professional bias towards the organizational and people aspects of this challenge.