The Temporal Dimension of Defending Forward

A UK perspective on how to organize and innovate to achieve US Cyber Command's new vision

Alan Mears | Joe Mariani

ABSTRACT

The 2018 DoD Defense Strategy seeks to deter and defeat adversaries through a policy of forward engagement.[1] The Strategy and the related USCYBERCOM Vision mark a significant change in how the US intends to contest the emerging complexity of cyberspace in an environment where the rules will be more restrictive for the US and its allies than those of adversaries. Recognizing an ingrained military culture of geographically driven maneuver warfare, it will be important that USCYBERCOM considers the temporal as well as the spatial elements required to defend forward. A combination of timely, better and more coherent-decision making across a pan-government and industry ecosystem must exploit rather than attempt to control chaos; the effective adoption and application of decisive innovative capabilities will be a related essential element of this strategy. Through a UK lens, this paper considers the temporal implications of a strategy of Defending Forward.

INTRODUCTION

A body of recent U.S. Government publications has outlined a significant shift in strategic thinking in the context of the changing geopolitical climate and cyberspace; for example the 2018 U.S. National Defense Strategy states that adversaries no longer respect established global norms, and are engaged in a constant state of espionage, disruption and shaping activities against the US, and its allies.[2] This is leading to increased competition across the full spectrum of Diplomatic, Information, Military and Economic (DIME) levers of national power. The UK's National Cyber Security Strategy and the International Institute for Strategic Studies (IISS) recognize the persistent and evolving cyber threat, manifested through such concepts as grey and tolerance warfare; these suggest that this emergent behavior is having an increasingly profound effect on our understanding of future threats to the prosperity and security of our nations.[3][4]

Adversaries are aggressively exploiting policy and decision-making frictions and boundaries of the US and its allies.[5] While this condition of constant competition falls short of overt conflict, it is all about out-maneuvering opponents. It is therefore essential that the US and the UK adapt their strategies and policies to both deter adversaries but also to seize and retain the initiative; Defend Forward should be approached as an active and not reactive strategy. Not to do so, or to do so too late, risks ceding the initiative entirely, as the Commander of U.S. Cyber Command (USCYBERCOM) has pointed out.[6] The 2018 DoD strategy seeks to address this and directs the Department to defend forward, shape the day-to-day competition and prepare for war by building a more lethal force, expanding alliances and partnerships, reforming the Department and nation, cultivating talent, while at the same time actively competing against and deterring competitors.[7]

Reflecting on this significant shift in emphasis, it is worth noting that much of the Defense community is culturally pre-disposed to apply positional context to operational problems. The traditional focus on maneuver tactics misses the importance of a campaign that shapes an adversary's political and economic networks to achieve a position of relative advantage.[8] Thus Defend Forward and "close to the origins" may lead to a tendency to focus on the physical dimensions of the concept. If traditional physical boundaries such as Joint Operational Areas (JOAs) are now less relevant, it will be important to consider how other elements such as timely and accurate decision making and the ability to develop and maintain a winning edge in the application of innovative capabilities might contribute to this strategy.[9] Against an understanding of related US and UK concepts and approaches being developed, this paper will consider some key temporal aspects that may contribute to the outcome of Defend Forward. Drawing on a review of available academic, policy and broader related literature, this paper will discuss the following:

- Briefly contextualize the requirement for Defend Forward
- Consider the temporal element as a contributing factor to Defend Forward
- Consider the role and possible approach to a coordinated pan-defense, government and industry trusted ecosystem
- Consider how concepts of anti-fragility and chaos might contribute to a decisive operating edge
- Analyze the key elements of the discussion to identify some key organizational principles and approaches that may contribute to the strategy of Defend Forward.

In considering these themes it is recognized that each is highly complex and worthy of more substantial analysis in their own right. The aim of this paper, however, is to introduce these as related themes to a broader audience in sufficient detail to demonstrate some key inter-dependencies and experiences that can contribute to the design and implementation of the future strategy.

DEFEND FORWARD IN CONTEXT

Military history demonstrates that the Commander who seizes and maintains the initiative dominates the adversary, and that defense properly conducted is a transitionary phase that provides a platform for decisive effect.[10] The Vision for USCYBERCOM, Achieve and Maintain Cyberspace Superiority, translates the National Defense strategy of Defend Forward into a cyberspace strategy of persistent engagement, a fundamentally new strategy for US cyber operations.[11] The Defend Forward strategy will require cyber operators to seize and maintain the initiative in cyberspace by continuously engaging adversaries and causing them uncertainty wherever they maneuver. The strategy requires continual and global operations, keeping as close as possible to adversaries and their operations. A defense of this kind will create operational advantage for the US on the battlefield while denying the same to its adversaries.[12] A number of significant implications are arising from this new approach that will need to be understood and addressed. Max Smeets highlights the degrees of collaboration and understanding the US will need to have with its allies if the US intends to conduct operations through or in their networks; there will be similar issues where these allies seek to operate over US networks.[13] In addition, critics of Defend Forward question the efficacy of such a strategy which they see as increasing the risk of escalation while doing nothing to make cyber operations more effective.[14]

As allies facing common trends, the UK thinking on cyber is moving in a similar direction to USCYBERCOM. While there is no direct UK Defence equivalent as yet to the USCYBERCOM Vision, the approach is well represented in a range of recent policies and approaches. The Joint Concept Note 2/18, Information Advantage, suggests that central to emerging strategic contests are “information battles” in which information is “weaponized” and where the UK and its allies increasingly lack the initiative.[15] These require UK Defence, as part of a national and allied effort, to become a potent and resilient strategic actor postured for constant competition both at home and away. The developing Capstone Concept for Strategic Integration (CCSI) suggests that simply doing more of the same is not an option, and reinforces the need to drive the conditions and tempo of strategic activity, instead of merely reacting to the actions of others; the paper highlights the need to be agile and to operate at pace continuously developing new ways and means to compete.[16] Similarly, reflecting the themes of the CCSI, the developing Integrated Operating Concept (IOpC) 2020 highlights the importance of a resilient home base as critical for any future operations, and the need for a unified and integrated cross-government Homeland Defence architecture to deliver this.[17] In developing approaches to support these initiatives, the Army’s concept of Information Maneuver stresses the importance forward engagement and the power of the narrative in an era of Constant Competition; it recognizes warfare in the information age as a multi-domain battle which will face increasing challenges to its technical superiority requiring an agile acquisition and support network capable of responding to changing operational needs.[18] Both the Royal Navy and the Royal Air Force are developing similar strategies; for example the Navy’s Project Nelson initiative is a dynamic experimentation program looking at the application of a range of technologies such as AI and Machine Learning, and its approach to the adoption of autonomous systems is being seen as an exemplar in NATO.[19]

Common to both US and UK visions for cyber operations is the requirement to stay consistently and continually engaged with networks, both social and physical, and problem sets beyond national borders. Naturally, this can lead to the idea that the new strategies simply expand the scope of cyber operations geographically, but the truth is that it also changes how cyber forces operate as well.

FORWARD IS TEMPORAL AS MUCH AS SPATIAL

Understanding and connecting the spatial and temporal elements of maneuver has been a critical element of the planning and execution of military operations throughout history. Given the global and instantaneous nature of the emerging cyberspace environment, connecting and exploiting the synergies of these elements will be an essential factor of Defend Forward. Untimely and poor decision-making can have profound implications for successful campaign outcomes. This does not necessarily require a faster Observe, Orientate, Decide, Act (OODA) loop, just the ability to act faster than the adversary which can be achieved by speeding up your own OODA loop, degrading that of the adversary, or more likely a combination of both. History provides multiple examples where appropriately forward-positioned forces have ended up in the wrong place through centralized or dysfunctional command and poor decision making. Reflecting on the 75th anniversary of D-Day, Allied success in Normandy, for example, was due in no small part to "fixing" forward-deployed, capable enemy formations in the wrong place through deception, sabotage and a lack of appropriately delegated authorities in the initial stages. Although the Germans were highly trained and skilled in counter-attack, they could not mount a successful defense.

Given the accelerating complexity and chaos of this environment, commanders will increasingly require flexibility and freedom, the agility to deal with rapidly changing demands. In these circumstances in may no longer be possible or even appropriate to plan or invest in the absolute detail of the layout or requirements of the future.[20] At the same time, relying on rapid response and reactivity may place challenging, if not impossible, demands on capability, thus there is a related need to invest in anticipation. This is not a new concept in the military where it is an established truth that although a plan rarely "survives contact with the enemy" it is only through this process that real insight and agility can be derived.[21] So the corollary of not having to react so quickly is that we have to take anticipatory steps much earlier, and shape activities to create the conditions under which problematic circumstances will either not arise, will be more benign, or can be more easily addressed.[22] Commanders will therefore have to focus on creating the conditions, through appropriate policy frameworks and direction, under which their subordinates can operate.[23] An important element of this approach will be the ability of USCYBERCOM to not only accept, but to embrace, chaos. Dee Hock, former president of VISA International used the term chaordic to describe the need for organizations to be both chaotic and ordered to achieve agility.[24]

Contributing significantly to this chaordic challenge is the added and perhaps unnecessary friction to timely decision making through the creation of the Fifth Domain of cyberspace.[25] In doing this, the US. the UK, and their allies have created another, almost separate community that needs to be integrated and de-conflicted alongside the planning and orchestration of other closely related capabilities such as Electronic Warfare (EW), Psychological Operations (PsyOps), and Information Operations (IO). In contrast, Keir Giles states that Russia sees "information confrontation" or "information war" as a broad and inclusive concept which contains computer network operations alongside disciplines such as PsyOps, strategic communications, influence, intelligence, counterintelligence, deception, disinformation, electronic warfare, and destruction of enemy computer capabilities. Giles describes this as forming a "whole of systems" in which the blending and coordination between different informational tools is a distinctive feature of how Russia aspires to prosecute information warfare.[26] The Chinese have a similar approach in their construct of Informationized Warfare.[27]

While chaos may allow initiative to flourish, at the same time it should be held within a system of overall cooperation if it is to enable rather than confound.[28] Across the Defense community the operational framework and the concept of Mission Command is designed to operate in such conditions that seek to combine subjective and objective behaviors to balance the art and the science of warfare.[29] Mission Command has its origins in the 18th Century concept of *Auftragstaktik* within which the basic premise is that commanders should give subordinates general direction of what is to be done, allowing them the freedom to determine how to do it.[30] This is reflected in the U.S. Army's ADP 3-0 Unified Land Operations and ADP 6 Mission Command, Command and Control of Army Forces, which require Commanders to enable adaptive forces through flexibility, collaborative planning, and decentralized execution; Mission Command is seen to maximize autonomy and foster individual, initiative thereby enabling force elements to act rapidly through enhanced flexibility and adaptability across the range of military operations.[31][32]

However, like any philosophy, Mission Command must be enabled if it is to deliver. In military operations, there is a growing tendency to limit initiative through overcentralized control and poor delegation. The ubiquitous nature of modern communications has further stifled Mission Command with strategic commanders able to tactically control the battle. This level of connectivity has also resulted in tactical actions that have much more of a strategic impact by being immediately visible to a global audience. In addition, the daily conduct of home based military activity does little to develop or foster the behaviors that underpin Mission Command; one has to question how the next generation of commanders will ever be comfortable with taking the responsibility such an approach requires when they are not routinely familiar with its application. Despite these issues, Mission Command is still the advocated approach and one that is taught and recognized across Defense, but there is no such equivalent framework that embraces wider DIME community. Given these tensions between enabling initiative and centralized control across Defense, there are significant challenges and frictions that will confront any attempts to apply a Mission Command approach across the broader DIME ecosystem.

ENABLING AN ECOSYSTEM FOR DEFEND FORWARD

Recognizing the importance of US Critical National Infrastructure (CNI) and the broader public and private sectors as components of the strategy to Defend Forward, a key aim of the 2018 DoD Cyber strategy is the need to preempt, defeat, or deter malicious cyber activity targeting US CNI. It also highlights the need to provide public and private sector partners with Indications and Warning (I&W) of malicious cyber activity, in coordination with other Federal departments and agencies. Given that conflict increasingly takes place across connected national societies that are inseparable from global networks, there are implications for militaries who depend on many of these networks as a minor user among many, thus opening up a Pandora's box of risks that now expose the very security and prosperity that Governments are investing in.[33][34] Not surprisingly adversaries have observed the opportunities of this connectedness and also the increasing trend of elevating responsibilities and authorities to higher levels of command; they have recognized that the challenges and frictions of cross-government decision-making have made our systems comparatively slower and less agile.[35] As former U.S. Secretary of Defense Ash Carter stated:

> The State Department, for its part, was unable to cut through the thicket of diplomatic issues involved in working through the host of foreign services that constitute the Internet. In short, none of our agencies showed very well in the cyber fight.[36]

This friction is reinforced by a lack of proportionate responses to deliberately escalating challenges which appear to be emboldening our adversaries.[37] If today's organizing principle is no longer sovereign territory but a new geography and resulting geopolitics organized around social networks and supply chains then, as Martyn suggests, security will be based on a team effort that not only requires constant vigilance, but a community oriented, proactive mindset.[38][39] A contributing feature in addressing this as identified by the Organisation for Economic Cooperation and Development (OECD) is the need for the wider diffusion of information among a larger number of workers. This increases the importance of management and co-ordination and the importance of a more horizontal work-based approach within digitally enabled workplaces. This requires teamwork rather than top-down management which in turn calls for more co-operation, collaboration and trust.[40]

But the priorities of boards and directors of the majority of organizations across the public and private sectors are naturally driven more by compliance and profitability than National Security considerations; they may have little understanding of their evolving status as potential targets for the political machinations of highly motivated and capable state-level actors, and even less for any additional expenditure on cyber defense which many view as a business loss.[41] Engaging these organizations as part of a coordinated National Security effort within a Defend Forward ecosystem will require a more holistic and collaborative understanding of the shared risks, and the initiatives to address them. General Sir Richard Barrons observed that the ability to shake the foundations of a population's morale and cohesion through skillful information-based manipulation means it is not always necessary to invade territory to break a state; this can be done decisively from long range, and he proposes an organizational structure to address this as illustrated at Figure 1.[42]

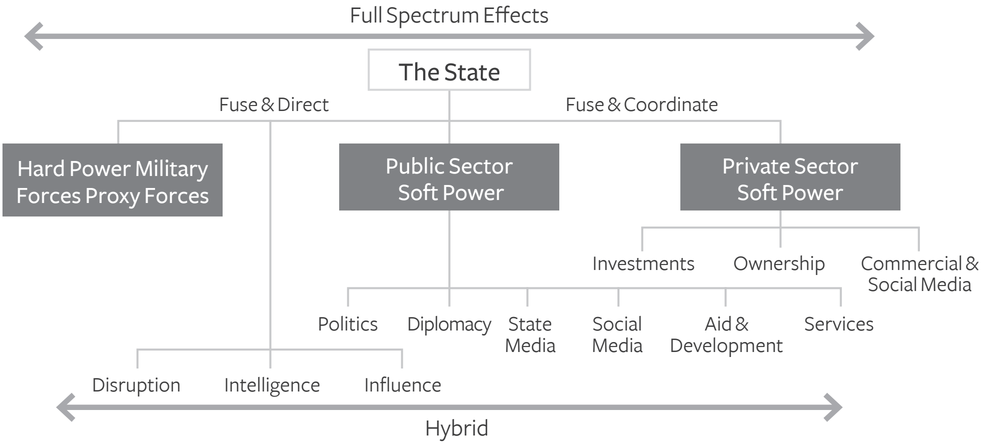

Figure 1: Success requires all levers of power [43]

UK efforts to address these particular challenges may provide some insights to USCYBERCOM. The development a new National Security doctrine, the Fusion Doctrine, is outlined in the National Security Capability Review (NCSR).[44] This seeks to improve the UK's collective approach to National Security and aims to use its security, economic and influence capabilities to maximum effect to protect, promote and project the UK's national security, economic and influence goals. In particular the Doctrine notes that many of the capabilities that can contribute to National Security lie outside traditional National Security departments and also demand stronger partnerships between the public and private sector and the international dimension where security, trade and development partnerships are often mutually reinforcing. This Doctrine will play a key role in the UK's approach to modern deterrence which will be conducted as a whole-of-government activity with the purpose of deterring catastrophic threats entirely.

There are significant cultural and organizational, as well as policy and technological challenges, which will need to be addressed within this strategy. Lacking the same immediacy of the threat as that for example perceived by the Baltic States, there is a limited appetite for the constraints and discipline necessary to deliver a policy of "Total Defence" to a population that is largely removed from the concept of the existential modern threat they face.[45] It is therefore evident that the complexity, and in many ways the near anarchy, of this complex ecosystem is unlikely to be addressed through an approach that relies on the rigid application of policies and statutes; the complexity and fluidity of the cyber domain combined with all of the social, cultural, organizational and legal challenges that are implicated will require the evolution of a DIME ecosystem that can orchestrate and enable the chaotic and anarchic nature of its components under a trusting and cohering purpose.

EXPLOITING ANTI-FRAGILITY AND CHAOS TO DELIVER AN OPERATING EDGE

Management science has known since at least the 1970s that faster, more responsive decision-making across complex organizations can result from delegation closer to the tactical edge, but this, in itself, creates its own tension as it is difficult to be sure that these decisions are coherent with the overall strategy.[46] The traditional management approach is to have a strategy, break-out operational tasks, then distribute those tasks to subordinate tactical workers for execution. This allows tactical workers to be sure that their actions are coordinated and aligned to the outcomes the executives have pre-determined. Unfortunately, organizations competing at the pace of change in the modern world are discovering that such an approach results in poorer outcomes. While many executives may still create their strategic plans, they do this annually, at best, their workforce operating at the tactical edge must respond to changes in the environment on an almost daily basis as illustrated at Figure 2.[47] This mismatch in the wavelength or periodicity of tasks at different levels stresses the structures of modern organizations and demands that decision makers be more agile.

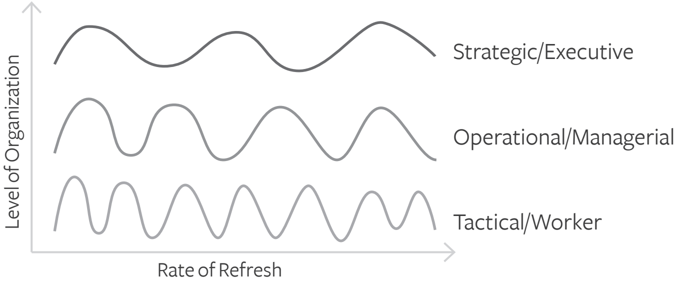

Figure 2: The "wavelength" of tasks in the modern world [48]

At the 2019 conference on Big Data for Defence in London the Chairman, General Andrew Sharpe, noted that:

> "whatever the technology, procrastinators will still procrastinate, idiots will still be idiots. We must organize to be comfortable with chaos as we move forwards".[49]

A clear inference that can be drawn from this is that mental agility and dexterity will be an important personal characteristic of decision makers in an increasingly complex environment where organizations will need not only accept, but to embrace, chaos within a system of federation and overall cooperation. Nassim Taleb suggests that complex man-made systems, such as the cyber domain, tend to develop runaway chains of reaction that decrease or even eliminate predictability causing outsized events. Paradoxically, the modern world, by increasing technological knowledge, is also making it more unpredictable.[50] Taleb also suggests that a tendency to take the present as a baseline and then produce a speculative future based on the addition of technologies, although in some ways logical, tends to over technologize the approach adding further to the complexity, and thus the unpredictability, of the outcomes; instead he advocates the value of self-learning and gives weight to those elements that continue to survive.[51] Taleb advocates the benefits of anti-fragility in the environment that is based around acceptance of the theory that corporate resilience derives from the recognition that federation is key and individuals are "unfit" components that should be allowed to fail if the corporation is to learn and progress. This approach, which encourages mistakes while also containing them, will succeed over one that tries to overcome failure through the over-centralization of control.[52]

In the military context, in his book Team of Teams, General Stanley McCrystal reflects on many of these issues as he describes how his own experiences in Iraq and Afghanistan forced him to change as a leader and, in the process, find a new way of structuring and leading organizations in the chaos of the modern technological environment. Speaking to Joe Mariani, he observed that the tipping point for him was the realization that whereas previously only the military had access to the scale and complexity of resources that allowed decisive decision making over less well equipped adversaries, that technology had become widespread, and instant communication had become available to everyone.[53] In addition, the sheer scale and complexity of data increasingly challenged attempts at sense-making within hierarchical and centralized Command and Control (C2) structures. What he discovered was the benefit of processing and exploiting information across the entire organization without tightly controlling that process, thus allowing everyone to think and have the information to allow them to act locally. The problem he faced with rapid change in the environment was the increased requirement for internal coordination or synchronization as the organization moved towards the chaotic as illustrated at Figure 3.

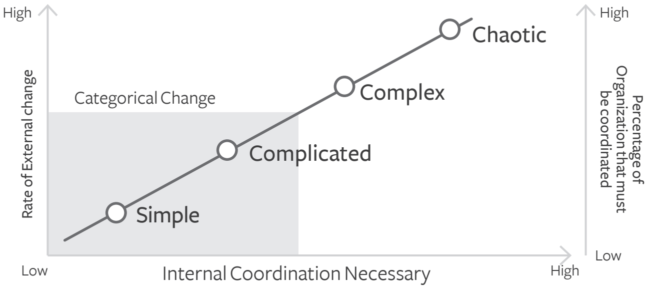

Figure 3: External change v Internal coordination [54]

A key deduction he drew from this experience, and relevant to the complexity of modern persistent conflict, was the need to develop and work within a concept of trust and a common purpose to address the complexities and be adaptive. This approach should be based on shared consciousness and empowered execution which will allow the necessary speed and interdependence required for the "edge" elements to act quickly and independently but within the overall intent.[55] This is illustrated at Figure 4.

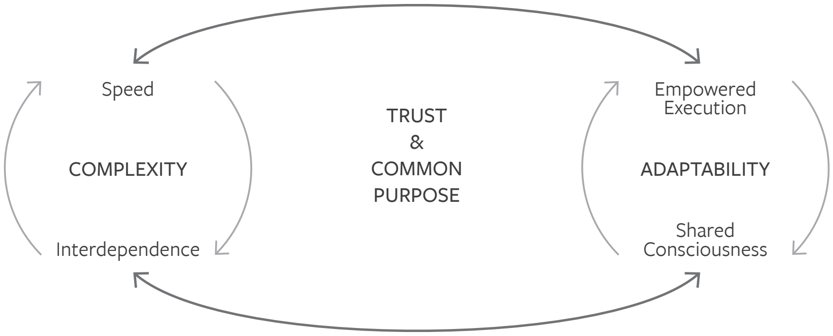

Figure 4: The role of Trust and Common Purpose in addressing complexity and chaos [56]

In the light of this discussion, it is evident that simply tinkering with current cultures and structures will be insufficient to deliver the vision of Defending Forward, and that a fundamental shift in organizational approach, culture and ethos will be required moving forward. Traditional notions that knowledge and wisdom are the preserve of the senior officer must adapt to a culture where leadership will embrace delegation, providing a cohesive vision. They should encourage and act in response to the advice and guidance of the most junior, non-commissioned junior officers and, where appropriate, non-military staff when they are clearly the experts.

DIFFERENT MISSIONS, DIFFERENT ORGANIZING PRINCIPLES

To understand how the issues discussed in this paper may inform future organizational constructs for USCYBERCOM, we need to understand the specific complexities that should be addressed as part of the new Vision. A deeper reading of the new Vision indicates that there are in fact different types of complexity and each one requires a different organizational structure. On the one hand, there is the need to constantly attend to the products and processes of the past, but at the same time, there is a need to explore the innovations that will define the future.[57] The Vision intends to be able to conduct multiple tactical to strategic level operations concurrently, while there is valid debate over whether or not it is possible to separate out tactical, operational, and strategic levels of conflict today, it is reasonable to assume that tactical and strategic cyber operations start at two different ends of a spectrum but will have substantial overlaps. These two differing drivers and conditions largely set the tone of the effects required with different, if perhaps supporting, goals and means. With different organizational forms being suited to different tasks, tactical and strategic offensive cyber may require different tools, teams, and structures to achieve the Defend Forward strategy. In order to execute these two concurrent missions, USCYBERCOM will need to organize to address two fundamentally different challenges concurrently: it will need agile cross-functional teams, enabled through a mechanism of delegation and trust combined with a common purpose to contest and succeed in today's fight and it will need to empower "practitioner" groups of planners and innovators, who will be plugged into large networks with the purpose of contesting and winning in the shaping and innovation space. This challenge of organizing to cover related but separate challenges is not uncommon in industry and is referred to as enabling the ambidextrous organization.[58] On one hand, USCYBERCOM will need to become a now-focused, rapid response organization composed of cross-functional teams able to anticipate and respond tactically to any contingency. On the other hand, it will need to be a future focused organization with small groups strongly linked to innovators bent on developing technologies and techniques that will provide the operational edge.

Looking at former, the challenge of organizing to anticipate and respond rapidly to changing tactical circumstances is perhaps the best known of the two activities to a military audience. Acting faster than adversaries on land, air, and sea has been the backbone of decades of military strategies. But just because it is familiar does not mean that the answers are always immediately apparent even to the best trained and equipped units. The lesson from McChrystal and Joint Special Operations Command (JSOC) is that having the right strategy, the right tools and even the right people may not be enough if you are asking them to operate within a poorly designed system, and that organizational structures need to be tailored to the outcome that an organization's strategy demands.[59] In order, therefore, to begin to organize to Defend Forward the key characteristics that will be required will need to include:

- Decision-makers with the necessary aptitude, mental agility and dexterity to understand and exploit opportunity
- Trust, a common purpose, and shared consciousness
- Delegated authorities and resources enabling the execution of operations to the edge
- Cross-functional teams focused on a common problem
- A focus on being a share-first organization to emphasize the flow of information between/among teams
- A change in the expectations of leaders from direct supervision to enablement
- An emphasis on developing a Mission Command orientated organizational culture so that leaders are more familiar with, and confident in, delegating to subordinates.

In turning to the latter, the strategic operations end of the spectrum, a temporal, maneuvering advantage can only be realized by achieving and sustaining a credible cyber advantage over the adversary and his capabilities. This has the implicit task of requiring USCYBERCOM to remain permanently at the cutting edge of adopting and applying cyber related capabilities through empowered and delegated policies and decision making. For example in early 1943, (and strongly encouraged by Winston Churchill and supported by Chief of the General Staff and his brother-in-law General Montgomery) General Percy Hobart was put in charge of the newly formed 79th Armored Division to cohere a specialized armor innovation and operational adoption across a range of armored "funnies" to support the D-Day invasion—the rest, as they say, is history. There was no similar initiative in the US and this stovepipe mentality prevented the widespread dissemination of this specialized vehicle development theory, development and fielding until well after the war's end.[60] Hobart's approach was one that was supported at the highest levels, had a cohering vision, and, while no idea was off the book, he took suggestions from all ranks.

While the National Defense Strategy states that:

> success no longer goes to the country that develops a new fighting technology first, but rather to the one that better integrates it and adapts its way of fighting", it is evident that today's top down hierarchical approaches are not geared to this challenge.[61]

The UK's Future Force Concept identifies innovation, greater automation and creative thinking as keys to sustaining freedom of action in the emerging Operating Environment; it describes innovation as threatening existing capabilities in which militaries have made heavy investment and have cultural baggage.[62] However, the evidence on both sides of the Atlantic points to long-established policies, cultures, processes, and structures that have a mixed record in facilitating rapid and innovative adoption, particularly in the areas of information technologies. Related to this, as identified by Klemas and Choucri, these frictions are further exacerbated by a struggling acquisition framework.[63] These were far from fit for the late 20th Century, and unaddressed will become a growing inhibitor in the operating environment of the 4th Industrial Revolution.

What is increasingly advocated is a collaborative and interactive innovation mechanism that places knowledgeable operators at the center rather than at the beginning and end of a dispersed development process. In considering the applicability of Early Synthetic Prototyping (ESP), Smith and Vogt point to concept developers, capability developers, scientists, and engineers who continuously interact with the operator.[64] This prototype of warfare concept will field many simple capabilities on a rolling basis, instead of a single, exotic one just once. Initially, a wide array of diverse prototypes will be developed and evaluated in experimentation programs. After, the particular prototypes that have proven successful in the trials will be produced in limited numbers and quickly introduced into service. A key element for success is the "Innovation Catalyst" who works within the senior leadership team and is demonstrably able to make change happen, and a fit for purpose and adaptive acquisition process.[65]

Professor Nina Kollars puts forth a similar argument when she suggests that there is no innovation without adoption, suggesting adaptation is a key element of military innovation. There are many examples of innovative, battle-winning capabilities that were never realized, and which represent a rhetorical capability, rather than a real one. An understanding of the roles of Grand Design (the crazy ideas and the paradigm shifts), the nature of improvisation, and the role of experienced and insightful practitioners are key to innovative adoption. Practitioners form the anvil on which potential can be forged:

> therefore, major military innovation requires the alignment of theory and practice—the marriage of the adaptation process with grand design.[66]

In order to engender an environment in which this approach to innovation might flourish, Professor Kollars also suggests that innovation and its sub-processes need both chaos and structure. Paradoxically, this requires a balance of independent action, interconnectedness, and hierarchy to make it possible for all to enjoy its benefits; there is clearly some resonance here with the concepts of chaos discussed earlier in this paper.

In addition, for USCYBERCOM to gain and maintain a cutting edge over its adversaries, it should embrace the widest possible breadth of talent possible through innovative career structures and harnessing the diverse talent pool of the broader community through close connections with industry, academia and allies.[67] These innovation hubs cannot be an ad-hoc, anarchic and a disconnected scattering of people across an organization. It will be critical that a constructive tension between a central brain and distributed and enabled hubs is realized through the appropriate connection between them and a shared understanding of a common purpose. The key characteristics that USCYBERCOM should therefore consider in addressing the right-hand temporal challenges to Defend Forward include the following:

- Anticipatory contingency planning to put in place the necessary enabling resources, policies and authorities and common purpose to enable rapid response
- Access to a wide range of talent
- A coherent, federated-but-connected innovation enterprise focused on exploiting the adaptability and adoption through practitioner-led participation; one that is plugged into the widest possible ecosystem of academics, industry, and allies possible
- Promotion of failure early in the process as a positive outcome to be rewarded
- An approach to live experimentation that develops and integrates the "good ideas" into adopted capabilities
- An agile and responsive and resourceful commercial and financial framework that delivers rapid prototype development and adoption within weeks as opposed to months or years.

CONCLUSION

The 2018 U.S. National Defense Strategy and the related USCYBERCOM Vision mark a significant change in how the US intends to contest the emerging complexity of cyberspace in an environment where the rules will be more restrictive for the US and its allies than for the adversary. The US should put in place the necessary conditions and capabilities that will enable the U.S. to overcome these constraints if it is to develop and maintain its advantage and Freedom of Action. Recognizing an ingrained military culture of geographically driven maneuver warfare, it will be important that USCYBERCOM considers the temporal as well as the spatial elements of its Forward Defense strategy. Using both a US and a UK lens, this paper has considered some of the temporal opportunities and challenges that can contribute to the strategy and suggested some cultural and organizational approaches that might help address them.

If the US and its allies are to learn from history, an approach that fails to recognize the temporal as well as the spatial factors will leave it dislocated and chasing shadows. They will need to realize that technological "advantage" is more a function of the application of "edge" capabilities through the faster adoption of winning solutions than simply the pursuit of new technologies. Enduring strategic advantage can only come from the close integration of process and technology and is driven largely by the manner in which practitioners, the people, are able to adapt to and integrate new capabilities. Since no individual organization can drive the development of every cutting-edge capability, USCYBERCOM should therefore look to place itself in an "innovation ecosystem." This ecosystem should include broader government, industry, the public and US allies and partners. Building and reinforcing the necessary collaborative policies and behaviors to achieve this should be a priority for USCYBERCOM and the U.S. Government. Transforming traditional hierarchical approaches to innovation and acquisition towards a more federated, connected, and agile organization will be essential to the US and its allies, if they are to compete at the same pace, let alone faster, than their antagonists.

But most significantly of all, if the US is to remain inside the OODA loop of the adversary, which it must do, it will need to embrace chaos and enable its "edge" organizations to fight today's fight within an understood and orchestrated strategy enabled by the necessary cultures, people, freedoms, and policies to act. Interestingly this is the very basis of Mission Command within the operational framework, a concept, which is more often than not, submerged under the constraining burdens of a lack of trust and risk-averse, centralized control.

Author Bios

Alan Mears

Alan Mears has over 40 years' service as a Regular and Reserve officer in the British Army and is an Associate Director in the UK Deloitte Cyber Security Risk Advisory team where most recently he filled an interim role as head of Cyber Security Assurance at Maersk. As an independent consultant he worked closely with the UKs Joint Force Cyber Group and the Cyber Joint User to develop the UK's MOD's Cyberspace Operations Ways of Working. In 2007 he set up the groundbreaking UK C2 Battlelab in Shrivenham where, working closely with deploying Brigades, he led efforts to "digitize" UK and NATO efforts into Afghanistan between 2007 and 2011. He was mobilized as SO1 Targets to IMEF for Operation Iraqi Freedom in 2003, and again to set up ISAF's Joint Fires and Targeting capability with HQ Allied Rapid Reaction Corps in 2006. Alan has an MSc in Cyberspace Operations from Cranfield University.

Joe Mariani

Joe Mariani leads research into defense, national security, and justice for Deloitte's Center for Government Insights. Joe's research focuses on innovation and technology adoption by both commercial businesses and National Security organizations. Joes' previous experience includes work as a consultant to the defense and intelligence industries, high school science teacher, and Marine Corps intelligence officer.

ACKNOWLEDGEMENTS

The authors thank the following for their contributions to this paper: Dr. Tel Venables of Tallinn University of Technology; Maj Gen Dr Andrew Sharpe CBE; Dr. Max Smeets of Stanford University; Jeremy Hilton; Cranfield University; Brendan Kober.

NOTES

1. Department of Defense, Summary of the 2018 National Defence Strategy of the United States of America. Sharpening the American Military's Competitive Edge, available at: https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf.
2. Ibid.
3. United Kingdom National Cyber Security Strategy 2016-2021, available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf.
4. IISS Strategic Survey 2018: The Annual Assessment of Geopolitics, Routledge, 2018.
5. Department of Defense Strategy for Operations in the Information Environment, P4, June 2016.
6. General P. Nakasone, A Cyber Force for Persistent Operations, JFQ 92 January 2019, available at: https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-92/jfq-92_10-14_Nakasone.pdf.
7. Department of Defense, Summary of the 2018 National Defence Strategy of the United States of America. Sharpening the American Military's Competitive Edge, available at: https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf.
8. Charles Cleveland, Benjamin Jensen, Arnel David, and Susan Bryant, Military Strategy for the 21st Century People, Connectivity, and Competition. Rapid Communications in Conflict and Security Series General Editor: Geoffrey R.H. Burn, Cambria Press New York.
9. Royal United Services Institute for Defence and Security Studies Occasional Paper, Peter Roberts, ed., "The Future Conflict Operating Environment Out to 2030,": https://rusi.org/publication/occasional-papers/future-conflict-operating-environment-out-2030.
10. Maj Gen (Dr.) Andrew Sharpe. Discussion with the author Jul 16, 2019.
11. Command Vision for US Cyber Command: Achieve and Maintain Cyberspace Superiority: https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010.
12. Ibid.
13. Max Smeets, "Cyber Command's Strategy Risks Friction With Allies," Lawfare Blog (2019): https://www.lawfareblog.com/cyber-commands-strategy-risks-friction-allies.
14. Brandon Valeriano and Benjamin Jensen, "The Myth of the Cyber Offense: The Case for Restraint," CATO Institute Policy Analysis No. 862, January 2019, available at: https://www.cato.org/publications/policy-analysis/myth-cyber-offense-case-restraint.
15. UK MOD, Joint Concept Note (JCN) 2/18, Information Advantage, November 2018, available at: https://www.gov.uk/government/publications/information-advantage-jcn-218.
16. The Capstone Concept for Strategic Integration (CCSI) The Defence Contribution as at February 2019.
17. Integrated Operating Concept (IOpC) 2020, September 3, 2019.
18. British Army Information Manoeuvre Conemp 2019.
19. Colonel Dan Cheesman, Chief Technology Officer, Royal Navy, IQPC Disruptive Technologies Conference, London, September 25, 2019.
20. Lorraine Dodd and Geoff Markham, "C2 Agility, Different Models of Change and Reasoning with Time," 17th ICCRTS: "Operationalizing C2 Agility" Paper 014, 2012.
21. Daniel J. Hughes and Harry Bell. Moltke on the Art of War: Selected Writings, 1993, 92.
22. Ibid.
23. Ibid.
24. Lee Dyer and Richard A. Schafer, "From Human Resource Strategy to Organizational Effectiveness: Lessons from Research on Organizational Agility," Centre for Advanced Human Resource Studies, Working Paper, (1998).
25. U.S. Joint Chiefs of Staff Joint Publication 3-12(R), Cyberspace Operations.
26. Keir Giles, NATO Handbook of Russian Information Warfare, Fellowship Monograph, Rome: NATO Defense College, 2016.
27. Timothy L. Thomas, Dragon Bytes: Chinese Information-War Theory and Practice, Ft. Leavenworth, KS: Foreign Military Studies Office, 2004.
28. Philip Boxer, "Working on the Edges," in *Asymmetric Leadership*: http://www.asymmetricleadership.com/category/centre-vs-edge.

NOTES

29. AJP-5, Allied Joint Doctrine for the Planning of Operations (Edition A), NATO Standardization Office, 2019.
30. John T Nelsen II, "Auftragstaktik: A Case for Decentralized Battle," Parameters, September 1987.
31. ADP 3-0 Unified Land Operations, Headquarters Department of the Army, 2011.
32. ADP 6 Mission Command: Command and Control of Army Forces, July 31, 2019
33. Myriam Dunn Cavelty, "Cyber-Security and Threat Politics" in CSS Studies in Security and International Relations, London, New York: Routledge, 2008.
34. Jose Nazario, "Politically Motivated Denial of Service Attacks," Cryptology and Information Security Series 3, The Virtual Battlefield: Perspectives on Cyber Warfare, Clifton: IOS Press, 2009, 163-181.
35. James E. McGhee. Liberating Cyber Offense. Strategic Studies Quarterly, Winter 2016, available at https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-10_Issue-4/McGhee.pdf.
36. Ash Carter, "A Lasting Defeat: The Campaign to Destroy ISIS," Belfer Center for Science and International Affairs, Harvard Kennedy School Report, 2017.
37. "Tolerance Warfare," IISS Strategic Survey 2018: The Annual Assessment of Geopolitics, IISS, 2018.
38. Royal United Services Institute for Defence and Security Studies Occasional Paper, Peter Roberts, ed, "The Future Conflict Operating Environment Out to 2030".
39. P. Martyn, Risky Business: Cybersecurity And Supply Chain Management, Forbes, 2017, available at: https://www.forbes.com/sites/gradsoflife/2017/08/18/more-than-whats-on-paper-how-gaining-independence-created-a-pathway-to-success/#299b02e11c14.
40. Organisation for Economic Cooperation and Development (OECD) and Mohammed Bin Rashid Centre for Government Innovation, Embracing Innovation in Government Global Trends 2017, Paris, OECD, February 2017.
41. Ibid.
42. General Sir Richard Barrons, note to Alan Mears, November 2018.
43. Ibid.
44. UK Government, National Security Capability Review, London: Cabinet Office, 2018, available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/705347/6.4391_CO_National-Security-Review_web.pdf.
45. Royal United Services Institute for Defence and Security Studies Occasional Paper, Peter Roberts, ed., "The Future Conflict Operating Environment Out to 2030," 2019, 9.
46. Herman Vantrappen and Frederic Wirtz, "When to Decentralize Decision Making, and When Not To," *Harvard Business Review*, December 2017.
47. Joe Mariani, "Leading to Chaos: A Conversation with General Stanley McChrystal," *Deloitte Review* 19, July 2016 available at: https://www2.deloitte.com/insights/us/en/deloitte-review/issue-19/general-stanley-mcchrystal-interview-innovation-in-leadership.html.
48. Ibid.
49. Major General (Ret.) Andrew Sharpe, Opening Remarks, Defence IQ Big Data for Defence Conference, London, June 25, 2019.
50. Nassim Nicholas Taleb, Antifragile: Things that Gain from Disorder, New York: Penguin Random House LLC, 2012.
51. Ibid, 313-315.
52. Ibid, 65-80.
53. Joe Mariani, "Leading to Chaos: A Conversation with General Stanley McChrystal," Deloitte Review July 19, 2016, available at:: https://www2.deloitte.com/insights/us/en/deloitte-review/issue-19/general-stanley-mcchrystal-interview-innovation-in-leadership.html.
54. Ibid.
55. Stanley McChrystal, Team of Teams: New Rules of Engagement for a Complex World, New York: Portfolio Penguin, 2015.
56. Ibid.
57. Charles A. O'Reilly III and Michael L. Tushman, "Innovation: The Ambidextrous Organization," *Harvard Business Review* (April 2004): https://hbr.org/2004/04/the-ambidextrous-organization.
58. Ibid.

NOTES

59. McChrystal, *Team of Teams.*
60. Major Michael J. Daniels, *Innovation In The Face Of Adversity: Major-General Sir Percy Hobart and the 79th Armoured Division (British)*, Pickle Partners Publishing, 2015.
61. Department of Defense, *Summary of the 2018 National Defence Strategy of the United States of America. Sharpening the American Military's Competitive Edge*.
62. UK MOD, J*oint Concept Note (JCN) 1/17, Future Force Concept*, September 2017: https://www.gov.uk/government/publications/future-force-concept-jcn-117.
63. Thomas Klemas, Nazli Choucri, Cyber Acquisition Policy Changes to Drive Innovation in Response to Accelerating Threats in Cyberspace, CYCON US 2018, available at: https://cyberdefensereview.army.mil/Portals/6/Documents/CyConUS18%20Conference%20Papers/Session2-Paper3.pdf?ver=2018-11-13-160900-057.
64. Dr. Robert Smith and Brian Vogt, "Early Synthetic Prototyping Digital Warfighting For Systems Engineering," *Journal of Cyber Security and Information Systems* Volume 5 no., December 4, 2017.
65. Thomas Klemas, Nazli Choucri, Cyber Acquisition Policy Changes to Drive Innovation in Response to Accelerating Threats in Cyberspace. USCYCON 2018, available at: https://cyberdefensereview.army.mil/Portals/6/Documents/CyConUS18%20Conference%20Papers/Session2-Paper3.pdf?ver=2018-11-13-160900-057.
66. Professor Nina Kollars, "Innovation is an Illusion," TEDx talk, Franklin & Marshall College, June 2016, https://www.youtube.com/watch?v=9UpAl0rmQ7o.
67. R. S. Burt, Martin Kilduff, and Stefano Tasselli, "Social Network Analysis: Foundations and Frontiers on Advantage,“ *Annual Review of Psychology* 64, 2013, available at: https://faculty.chicagobooth.edu/ronald.burt/research/files/SNA.pdf.