Deloitte.

Defensive Cyberspace Operations (DCO):

Contesting cyberspace

MAKING AN IMPACT THAT MATTERS since 1845

Contents

Defensive Cyberspace Operations (DCO): the need to move beyond cyber security

Introduction

Recent global geopolitical events have highlighted the pivotal role that information and cyber operations play as part of orchestrated strategic, operational and tactical campaigns. The ability to deny, disrupt and dislocate the understanding and decision making of nation states, their defense organizations, and the broader global interconnected communities enables the Freedom of Action required by military organizations to isolate and prosecute their strategic aims on the battlefield.

It is of note that there is nothing unexpected in this approach. A plethora of defense and academic papers and publications, and both current and previous confrontations, have continued to emphasize how states have been adapting their force structures and approaches to fully embrace and apply cyber and informational capabilities. As evidenced in past and ongong conflicts, we see today's strategic context as a continuous struggle in which non-military and military instruments are used unconstrained by any distinction between peace and war: there is an increasing focus on the contest to disrupt, paralyze, or destroy the strategic and operational capability and engagement of the adversary's operational system, described variously as Information Confrontation, Systems Confrontation and System Destruction Warfare.

More of the same will not suffice – rethinking is no good without action

This contest is not an equal one: whilst most nations may abide by accepted global norms and regulations, there is mounting evidence that others are no longer constrained by such ideas and work outside these accepted rules. Such behavior generates strategic asymmetric disadvantage for states who constrain their actions to these accepted norms of behavior; it is critical that states recognize, understand and mitigate the strategic and operational disadvantages of such a position. Within this operating environment, advantage in cyberspace is now a critical enabler for adversaries who wish to gain and maintain their influence and power over one another across the Diplomatic, Information, Military and Economic (DIME) arena; it must be contested at all levels through the coherent and determined orchestration of national strategic and military effects.

What is missing in this narrative is any pragmatic evidence that many nations have grasped the centrality of cyber capabilities, electronic warfare and algorithmic warfare[1] as part of the modern multidomain national defense capability set; they are failing to implement the organizational, cultural and capability changes required to provide for defensive operational capabilities in this new domain of operations. Established military domain centric and kinetic focused cultures continue to dominate; this is delivering risk averse and incremental change. The shortcomings of this are being amplified by adherence to acquisition policies and approaches that have already been criticized for their failures in delivering traditional platform capabilities; these approaches are even less suited for today's informational contest. Critical to this operating environment is the ability to defend the cyber domain to support and enable operations across each of the other domains. Building on a solid base of cyber awareness and cyber security, effective and orchestrated Defensive Cyberspace Operations (DCO) are now a key element of all operational planning and activity, and must be embraced and enabled through transformative change in defense organization and culture.

> Established military domain centric and kinetic focused cultures continue to dominate; this is delivering risk averse and incremental change the effects of which are being amplified by adherence to acquisition policies and approaches that are already recognized as failing.

[1] Algorithmic warfare is warfare conducted through artificially intelligent means. Artificially intelligent means are those that are not only intelligent (collecting and applying insight) but also artificial (acting on intelligence in a way that humans cannot).

"Important as bombs and missiles are, the synchronised and constant manipulation of all forms of communication: political; diplomatic; state, commercial and social media; paid-for influence; and expert cyber intrusion is now a daily part of how states compete, confront and conflict. For some, there are few constraints and no obligation to value the truth in prosecuting "full spectrum" information activity. Liberal, values-based, law-abiding democracies are at a disadvantage here. "Fake news" is just a taster of what harm can be done through pervasive information manipulation used against open societies as a weapon of war".

General Sir Richard Barrons

DCO is not just about IT and networks

As Defense forces struggle to take advantage of the transformative opportunities offered through this constantly changing technological miasma, it is critical to recognize that the digital and informational battlespace goes beyond simply IT systems and networks.

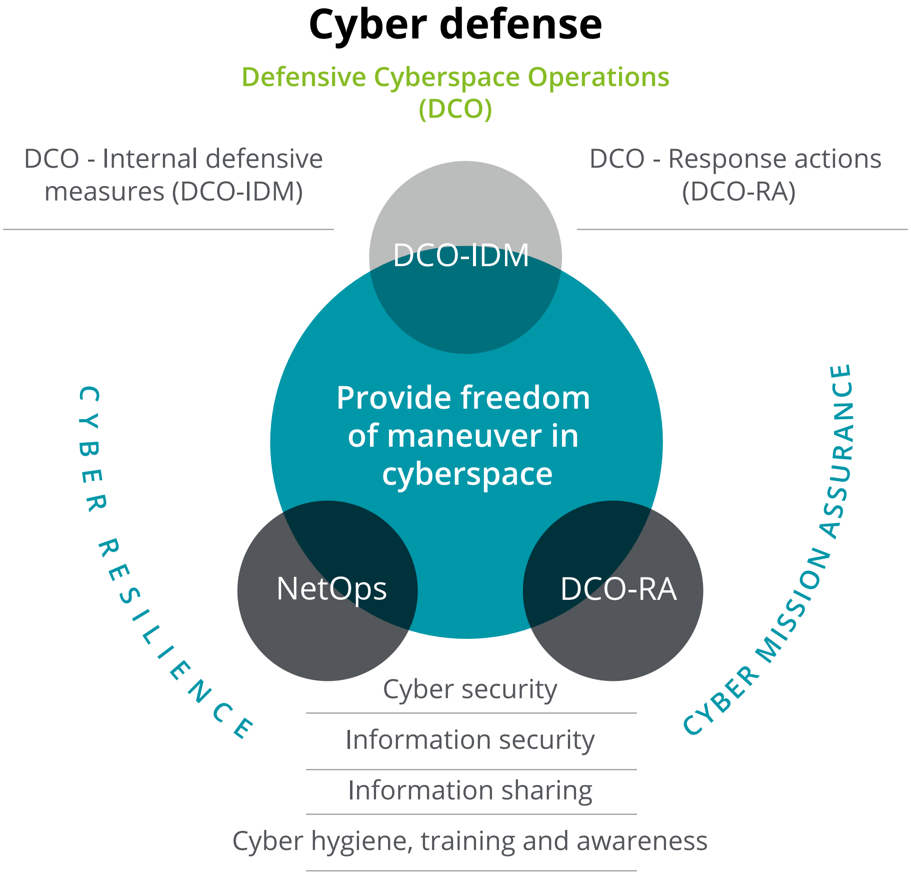
Commanders will increasingly only be able to effectively execute operations when the entire range of their networks, sensors, Command and Control (C2), logistic and weapon systems have been designed, built, configured, secured, operated, maintained and sustained with this in mind. This System of Systems (SoS) is increasingly the focus of belligerents seeking asymmetric and often inconspicuous opportunities to conduct espionage, and to disrupt and destroy the ability of their adversaries to plan and execute their operations with the confidence that their systems are capable of performing as designed or intended. The commercialization of space is accelerating and adding additional complexity to this ecosystem. Traditionally, defense and security efforts in space have centered on Precision, Navigation and Timing (PNT) and velocity. These must now be expanded as commercial and defense organizations embrace the Intelligence, Surveillance and Reconnaissance (ISR), networking and weaponization opportunities this domain provides. These SoS now represent capabilities that generate asymetric threats and opportunities which are already being tested and exploited. Space now represents a Centre of Gravity (CoG) and key terrain for defense and national security domains: "cyber defense "will be a principal focus area of the United States Space Force as we move forward."

This ecosystem of networks and platforms must therefore be safeguarded against information theft, manipulation, damage and destruction through determined and orchestrated DCO.

Key DCO concepts

It is impossible to fully employ today's joint force without leveraging cyberspace: commanders must develop the same capability to direct operations in the cyber domain since mission success increasingly depends on freedom of maneuver in cyberspace. At the top level, Cyberspace Operations (CO) center on the planning and orchestration of activities in and through cyberspace to enable Freedom of Maneuver (FOM) to achieve national and military objectives. These activities will include physical as well as non-physical actions and will both shape and support the multi-domain selection and execution of relevant operational Courses of Action (CoA). All CO are enabled through the appropriate and integrated application of Cyber ISR and Operational Preparation of the Environment (OPE).

Figure 1: The DCO landscape


Cyber defense
Defensive Cyberspace Operations (DCO)
DCO - Internal defensive measures (DCO-IDM)
DCO - Response actions (DCO-RA)
DCO-IDM
Provide freedom of maneuver in cyberspace
NetOps
DCO-RA
CYBER RESILIENCE
CYBER MISSION ASSURANCE
Cyber security
Information security
Information sharing
Cyber hygiene, training and awareness

A sub-set of CO, DCO seeks to deliver active and passive measures to preserve the ability of commanders to use cyberspace; these measures apply both in "peacetime" Business as Usual (BAU) and on operations. The purpose of DCO is to halt adversary offensive initiative, sustain or regain friendly initiative, and, if required, create conditions for a counteroffensive. It is not solely defined by the specific effect created or the capabilities employed. Passive defense activities, Internal Defensive Measures (IDM), represent the range of threat specific defensive measures and activities that can be undertaken to create resilience by reducing the effectiveness of adversarial cyber activities within our own SoS ecosystem. Active defense, Response Actions (RA), on the other hand seeks to preserve FOM within cyberspace by disrupting hostile offensive cyber capabilities and operations generally beyond our own SoS ecosystem.

A key precursor for successful DCO is the planning and integration of military deception (MILDEC) actions. Beyond simply creating "cyber honeypots" deception comprises actions executed to deliberately mislead the decision makers of adversary military, paramilitary, or violent extremist organizations, thereby causing the adversary to take specific actions (or inactions) that will contribute to the accomplishment of the friendly mission. DCO deception activities support the full range of offensive and defensive actions, across the physical, virtual and cognitive dimensions of cyberspace, and must be planned accordingly.

Similar to air-power, control of cyberspace will not be a permanent state and constant activity is required to achieve it. To gain and maintain the required advantage in cyberspace, DCO operations will be necessary to disrupt, degrade, deny or destroy an adversary's ability to challenge such control. This will require the coherent coordination and synchronization of Offensive Cyberspace Operations (OCO) and DCO missions with other informational and physical capabilities across all Lines of Operation (LoO); these actions must be planned and fully integrated with those of other environments to deliver Mission Assurance. DCO thus extends beyond the boundaries of the Defense enterprise and must consider external mission vulnerabilities delivered through transient dependencies on third party factors such as Critical National Infrastructure (CNI), the supply chain, partner nations, commercial logistics, and defense of the narrative and social support against disinformation.

DCO will require the coherent coordination and synchronization of Offensive Cyberspace Operations (OCO) and DCO missions with other informational and physical capabilities across all Lines of Operation (LoO); these actions must be planned and fully integrated with those of other environments to deliver Mission Assurance.

A focus on resilience and mission assurance

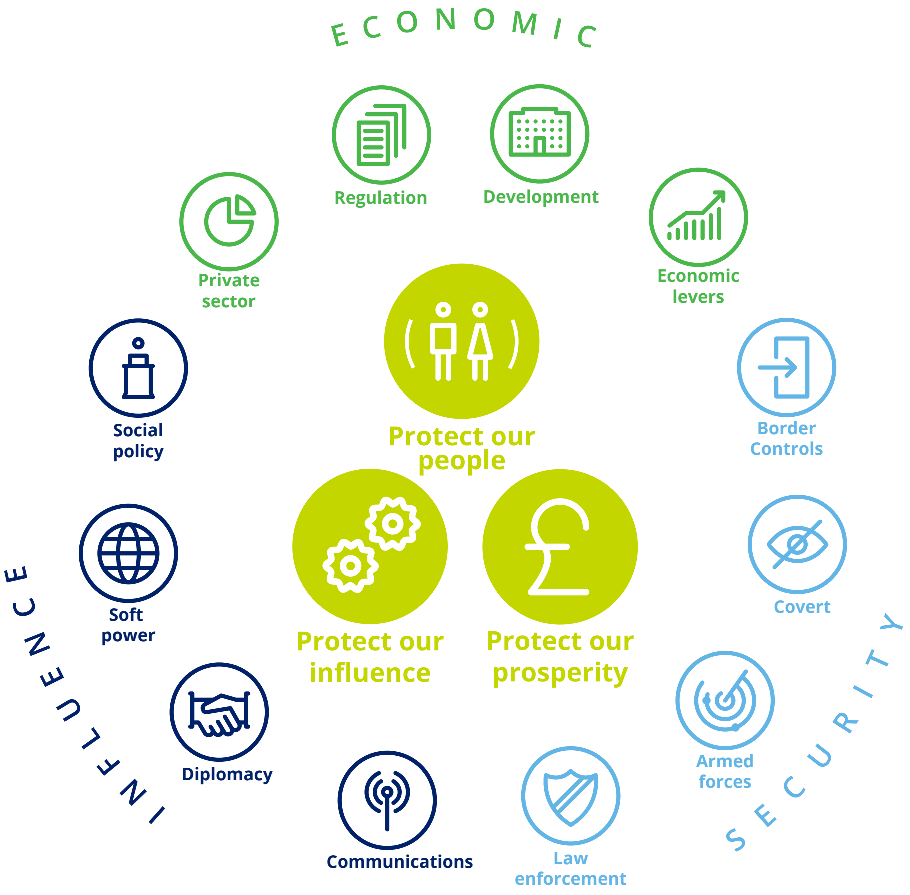
Rule number one in DCO is the recognition that the adversary is in your networks and in your SoS. Any sense that you can stop your adversary accessing, maneuvering through and disrupting your ecosystem is naïve; a focus on Defense ecosystem resilience will be of paramount importance. DCO will be a persistent contest of covert and overt physical and non-physical proactive actions to secure and maintain advantage and consequently FOM. These actions will be global, persistent, and generate multiple-dilemmas simultaneously. This convergence of global reach and multiple challenges will be compounded by developments in hypersonics and AI; these will exacerbate already problematic cognitive and decision making dilemmas facing commanders who seek to gain advantage through the application of a maneuverist approach to operations. Although emerging thinking challenges the accepted emphasis defense forces place on the maneuverist approach, and FoM it generates, this remains at the heart of operational planning and execution. This approach seeks to enable the required Freedom of Action (FoA) commanders require to seize and retain the initiative. Within this framework, Mission Command is the approach that underpins the maneuverist approach; it is based on the principle of centralized planning and decentralized execution that promotes maximum FoA and initiative, and grants subordinate commanders freedom in the way they execute their missions. The accelerating pace and complexity of the multiple-dilemmas that can be generated from the strategic to the tactical levels will be exacerbated by the use of Machine Learning and AI; the effective enablement and application of the principles of Mission Command to address these challenges will be critical to effective DCO.

> Rule number one in DCO is the recognition that the adversary is in your networks and in your System of Systems

However, achieving an enduring superiority or dominance in the information and decision making terrain is not achievable. A short-term competitive advantage, to achieve temporary advantage in order to enable military action, is a more realistic objective; this must be delivered through an approach framed by the required operational outcomes and driven by a focus on prioritization, collaboration, anticipation, resilience and agility. Adapting to changing complex environments, rather than seeking to control them, will be fundamental. A constant focus must be on defending and maintaining those most critical capabilities and audiences across the dimensions of DIME required to deliver the assurance that the broader strategic and operational mission outcomes will be achieved. As illustrated in Figure 2, this represents a complex ecosystem of economic, security and influence opportunities to any belligerent where the effective disruption of any combination of vectors represents the opportunity to disrupt a state's national, strategic and operational outcomes.

This concept, referred to as Mission Assurance, is defined as a process to protect or ensure the continued function and resilience of capabilities and assets, including personnel, equipment, facilities, networks, information and information systems, and infrastructure and supply chains critical to the execution of mission-essential functions in any operating environment or condition. Concentrating on the Tactics, Techniques and Procedures (TTPs) that orchestrate DCO to deliver Mission Assurance as part of this broader joint and multi-domain battle will frame the Mission, Task and Purpose of all operations through cyberspace.

Figure 2: The economic, influence and security dimensions of cyberspace



Cyberspace Operations represent a combat arm – they create decisive effects

As we have described, DCO will be conducted within the "operational framework" which comprises shaping, decisive and sustaining actions underpinned throughout by continuous understanding. Within this framework, and similarly to armor, infantry, artillery aviation and air, cyber capabilities can be used for ISR and to deliver shaping and decisive effects across the other four domains of maritime, air, land and space. This will require a shift in the skills and imagination of commanders who must now ensure that their planning processes recognize the need to build operational plans and potential Courses of Action (CoA's) that will be cyber and informational led as opposed to purely supporting or enabling activity. To achieve this, commanders at all levels will need to develop a deep understanding of the cyber and informational capabilities that they can employ as part of a coherent joint and multi-domain contest, and the opportunities and constraints that these capabilities will generate.

This will require a fundamental review of the skills and training of both cyber specialists and the generalists across defense; CO and DCO must be business outcome and not technology led. To date cyber has been the realm of information and cyber technologists and intelligence and security organizations. IT services are in the main provided by specialist organizations and individuals whose training and education omits roles as operational planners in the J3, J35 and J5 combat functions; their experience is largely requirement and response focused and quality of service driven using such frameworks as PACE and ITIL. Similarly, the culture of intelligence organizations is framed around secrecy and the need to know; this is profoundly problematic in that the warfighters will only ever use that with which they are familiar and trust; in addition "the need to share" information is a foundational requirement of effective cyber security and DCO.

At the same time, the traditional warfighter community such as the aviator, seaman, infantryman and the "tankie" have continued to protect themselves from the complexities and taxonomy of modern data, IT and cyber systems. Holding fast to the principle that these can be categorized as "supporting" elements where specialists can weave in their magic in the background and in accompanying annexes of the Operational Order, this community is failing to engage with and lead, a critical strategic, operational and tactical capability. It is no different from the journey from horse to tank, and the recognition and integration of air capabilities.

DCO will require a fundamental review of the skills and training of both cyber specialists and the generalists across defense; CO and DCO must be business outcome and not technology led.

The DCO vision and outcomes should be realized through a Cyber Defense Program which has the appropriate levels of delegated governance and resourcing to enable agile and courageous capability development and delivery

Where to begin – separating the wheat from the chaff

DCO presents a wide range of often conflicting opportunities to Defense; the challenge is to identify where to start. Whilst it is tempting to grasp at some low hanging fruit, often in the form of technology or tactical organizational changes, such an approach will simply delay and confuse the delivery of a coherent, resilient and relevant capability moving forwards. Whilst there are several initiatives that will be required, there are three key actions which should be addressed as a priority.

Initiative 1: Agree a multi-domain DCO vision and outcomes, and build the roadmap.
DCO must be designed to deliver cyber domain capability as part of an orchestrated and integrated joint and multi-domain activity. Without an agreed vision and agreed outcomes to deliver this, even the boldest of ambition will struggle to build and maintain momentum, coherence and purpose. This vision must be operations focused but be designed around a federated architecture and ecosystem that extends beyond defense to include other government departments and agencies, industry and partners. The vision and outcomes should be realized through a Cyber Defense Program which has the appropriate levels of delegated governance and resourcing to enable agile and courageous capability development and delivery. Ownership of this initiative should be at the highest level.

Initiative 2: Transform the workforce.
Without the right skills and culture, DCO will simply be a portfolio of constantly changing and disconnected technologies and activities that will leave gaps that the sophisticated adversaries of today will exploit with ease. Cyber is just one component of the broader digital transformation that impacts the full spectrum of defense capabilities that includes weapons platforms, ERP systems, C4ISR systems and logistics systems and the supply chain. Planning and delivering DCO capabilities require a combination of transformed "generalist" expertise adept and confident in the application of digital and cyber capabilities in the planning and execution of operations, and the broadening of specialist skills beyond cyber into the broader digital space of for example IT, AI and data. Without addressing the generalist requirement, cyber will simply sit on the shelf and its potential will be underused; without broadening the specialist skills individuals, and as a result Defense, will be unable to develop and retain the spectrum of DCO specialist and leadership skills that will be required to contest the digital battlespace. Prioritizing the cultural needs that will enable such a transformation will be pivotal to generating momentum.

DCO capabilities require a combination of transformed "generalist" expertise adept and confident in the planning and execution of operations and the broadening of specialist skills beyond cyber into the broader digital space

Defense must move away from concepts based on boundary and largely static technological defense to one that is focused on enabling resilience through adoption of cloud, dynamic and adaptive security capabilities, and a Secure by Design approach

Initiative 3: Resilient by design.
The rapid pace of change in digital capabilities and technology, is creating new and complex challenges for how the MOD contests the modern digital centric Operating Environment (OE) across all domains, land, sea, air, space, and cyberspace. These technologies, such as automation, data analytics, Artificial Intelligence (AI), Autonomous Vehicles, super and edge computing will transform Defense. They rely on huge amounts of data and compute power, seamlessly accessed via the Cloud and secured in such a way that this data can be relied upon and trusted. In order to successfully contest this complex space, Defense must move away from concepts based on boundary and largely static technological defense to one that is focused on enabling resilience through adoption of cloud, dynamic and adaptive security capabilities, and a Secure by Design approach:

- **Cloud:** Cloud based services are required across the whole of the defense enterprise in support of the full portfolio of defense use cases; these range from management information, medical services, Open Source Information (OSINF), logistics through to C4ISR, Joint Fires and Command and Control (C2). Understanding the requirement to connect and enable the movement, Confidentiality, Integrity and Availability (CIA) and innovation of data across multiple and dynamic Cloud Communities of Interest will be pivotal to the architectural approach that will be needed to support any defense Cloud future demand. Whilst a number of nations have embarked on this journey, such as the US and NATO, the nature of the challenges and future design of such a capability for Defense is still emergent. In particular, the needs of Defense organizations place requirements that extend the current application of Cloud services in commercial organizations: Defense organizations will have specific needs and challenges that will need to be understood and addressed in order to define and agree a target design architecture and implementation plan for its future Cloud needs. The ability to seamlessly connect these different deployment instances, whether remote, tactical systems, national and regional datacenters or Hybrid Cloud environments, into a common and resilient Data Fabric will be key[1].

[1] A data fabric is an architecture and set of data services that provide consistent capabilities across a choice of endpoints spanning hybrid multiCloud environments. It is a powerful architecture that standardizes data management practices and practicalities across Cloud, on premises, and edge devices. Among the many advantages that a data fabric affords, data visibility and insights, data access and control, data protection, and security quickly rise to the top.

- **Dynamic and Adaptive Security:** The implication of cloud architectures and computing has fundamentally broken that traditional defense in depth models that championed a strong castle and moat philosophy where boundary defense and edge protection and air gapped designs were deemed sufficient to defend against cyber threats. The reality is that data has rarely been static and behind the firewall. Defense entities must look beyond encryption and historical data protection and tactics. Modern computing architectures must be designed to not only be adaptable, but also resilient in the face of the growing cyber threat capabilities that the DCO faces. Concepts such as Zero Trust Architecture help ensure that data and services are resilient and protected from breach, service outage and data loss. Zero Trust is a concept that upends the traditional defensive order which used trusted enclaves into a design that treats all users, devices, services, applications, and networks as untrusted. This enables point to point protection through identity focused authentication and authorization and micro segmentation of networks and services. In this new paradigm, cloud architectures coupled with zero trust gives DCO an unparalleled ability to enable stronger and more resilient protections, but also enable more discrete monitoring and detection of unfolding threats.
- **Secure by Design:** A principle of Secure by Design delivered through approaches such as DevSecOps will combine key attributes of innovation with secure but rapid capability deployment. To support this Defense cybersecurity designs must incorporate Zero Trust principles to ensure protection closer to the data and include robust Identity, Credential, and Access Management (ICAM) to drive out anonymity and enable the secure sharing of information. Zero Trust solutions must control user activity within emerging Cloud-enabled cyber terrain. In coordination with the key national agencies, such as the NCA in the US and NCSC in the UK, they must also facilitate the deterrence, disruption, or the defeat of hostile red actors in cyberspace. To expand use of Cloud, defense must transition from an extant periodic Authority to Operate (ATO) approach towards one of continual monitoring and updating. Security will need to be automated to the maximum extent possible and leverage advanced Cloud capabilities such as AI to provide high reliability and assurance without excessive cost or administrative burden.

Conclusion

Today's Defense and Security environment is characterized by a continuous contest across the internet which has moved from a state of instability to stability as it has transformed into the modern powerhouse for digital commerce. As a result this global battlefield is now contiguous and the information across it is contagious. The internet is the pre-eminent communications medium that underpins defense, security and commerce in an inter-twined, and interconnected but ungoverned ecosystem. The internet is now vital ground for national prosperity and security: whoever manipulates it most effectively gains advantage across the battlefield, even if this is temporal.

DCO represent the critical, pervasive and decisive enabling activities and actions that are now critical to contest this key battlespace from the strategic to the tactical. However, DCO progress is slow despite the increasing application and effectiveness of offensive cyber capabilities as part of a coherent multidomain activity, as evidenced in recent geopolitical tensions and conflicts.

Whilst advancement in technological cyber security capabilities is big business and is evolving at an accelerating pace, a continued failure to address the profound cultural and organizational issues that underpin effective multi-domain CO and DCO will continue to be a fundamental barrier to the effective integration and application of cyber as a warfighting domain of operations.

It is now essential that defense organizations reorganize to enable the conduct of effective DCO, and operational planners at all levels become familiar with, and confident in, the integration and application of CO and DCO. This requires a shift in design, culture, organization, education and training where cyber proficiency and success is recognized and military awards and medals are equally applicable to decisive and courageous informational and cyber actions as they are for physical combat. Without this incentivization the war fighter will continue to focus on physical as opposed to informational career and professional development, and adversaries will increasingly dictate operational outcome.

Military awards and medals must become equally applicable to decisive and courageous informational and cyber actions as they are for physical combat

The internet is now vital ground for national prosperity and security: whoever manipulates it most effectively gains advantage across the battlefield, even if this is temporal

Contacts

Alan Mears is a senior advisor with Deloitte Middle East with over 40 years of service as a Regular and Reserve officer in the Royal Artillery and the Royal Signals. With a strong background in joint fires, cyber, targeting and C4ISR, Alan has over 30 years of experience in designing, delivering and executing joint fires C4ISR and cyber effects into operations. He was mobilized as SO1 Targets to IMEF for Operational 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.

Wayne Loveless is a senior advisor at Deloitte Risk Advisory in the Cyber Risk Services practice for Deloitte Middle East. He supports organizations improving their cyber risk posture through security initiatives that integrate strategic risk, regulatory, and technology components. Wayne has been leading projects on Cyber Security Strategy, Information Security Management Program, Risk Management, Security Assessment, Certifications ISO/IEC 27001, ISO 20000, and PCI, Implementation of Security Operations Center (SOC), CERT, Compliance, Data Loss Prevention, Digital Identity, Identity and Access Management, Business Continuity, and ICS Security.

This publication has been written in general terms and therefore cannot be relied on to cover specific situations; application of the principles set out will depend upon the particular circumstances involved and we recommend that you obtain professional advice before acting or refraining from acting on any of the contents of this publication.

Deloitte & Touche (M.E.) LLP ("DME") is the affiliate for the territories of the Middle East and Cyprus of Deloitte NSE LLP ("NSE"), a UK limited liability partnership and member firm of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL").

Deloitte refers to one or more of DTTL, its global network of member firms, and their related entities. DTTL (also referred to as "Deloitte Global") and each of its member firms are legally separate and independent entities. DTTL, NSE and DME do not provide services to clients. Please see www.deloitte.com/about to learn more.

Deloitte is a leading global provider of audit and assurance, consulting, financial advisory, risk advisory, tax and related services. Our network of member firms in more than 150 countries and territories, serves four out of five Fortune Global 500® companies. Learn how Deloitte's approximately 300,000 people make an impact that matters at www.deloitte.com.

DME would be pleased to advise readers on how to apply the principles set out in this publication to their specific circumstances. DME accepts no duty of care or liability for any loss occasioned to any person acting or refraining from action as a result of any material in this publication.

DME is a leading professional services firm established in the Middle East region with uninterrupted presence since 1926. DME's presence in the Middle East region is established through its affiliated independent legal entities, which are licensed to operate and to provide services under the applicable laws and regulations of the relevant country. DME's affiliates and related entities cannot oblige each other and/or DME, and when providing services, each affiliate and related entity engages directly and independently with its own clients and shall only be liable for its own acts or omissions and not those of any other affiliate.

DME provides audit and assurance, consulting, financial advisory, risk advisory and tax, services through 27 offices in 15 countries with more than 5,000 partners, directors and staff.