FORSVARSAKADEMIET

BRIEF

Battlespace Agility 201:
The OODA Moment

By William Mitchell, Ph.D.

FORSVARET

FORSVARSAKADEMIETS FORLAG

BRIEF

Battlespace Agility 201:
The OODA Moment

By William Mitchell, Ph.D.

The Royal Danish Defence College is the Danish armed forces' powerhouse for education, training and research-generated consultancy. Our research is conducted within a broad range of military-related topics. Our research priorities, such as topics and resource allocation are determined by the Commandant of the Royal Danish Defence College, who is aided by a research council.

Research at the Royal Danish Defence College should enlighten and challenge the reader, whether they are in the armed forces or in the surrounding environment. This is only achievable if the employees have the freedom to administer their own research projects and draw their own conclusions. This is a principle, which is honoured at the Royal Danish Defence College.

We hope you enjoy reading the Royal Danish Defence College's publications!

Copenhagen February 2013
Royal Danish Defence College
Ryvangs Allé 1
DK-2100 Copenhagen
Denmark
Phone: +45 3915 1515
Fax: +45 3929 6172
Editor: Oberstløjtnant Hans Henrik Møller
Layout by B-O. Kure
ISBN: 978-87-7147-018-5

Royal Danish Defence College Publishing House

Introduction

Battlespace agility is a warfighting concept defined as *the speed at which the warfighting organisation is able to transform knowledge[1] into actions for desired effects in a battlespace.*[2] In the brief *Battlespace Agility 101*[3], the importance of shared situational understanding between the Commander, the intelligence cell, and the operational planners was highlighted.[4] The purpose of this brief is to illustrate how *cyber technology*[5] has increased battlespace agility by dramatically increasing the tempo of decision-making using US Col. John Boyd's 1970's "Observe - Orient – Decide –Act" (OODA) loop[6]. Today, situational awareness and understanding[7] can be delivered to the operational decision-makers faster than at any previous period in history. Cyber technology does so through networks[8] of many different constructions, from fibre optics and electromagnetic waves, to other space based systems, including the wide application and integration of GPS[9] systems. For the purposes of this short brief, cyber technology refers to the use of the internet, computer, and network based communication and the technology developed from the convergence of computer and telecommunications networks.[10] Furthermore, though I am an experienced end user of a wide variety of cyber driven technologies, I am not a cybernetic technician.

Undoubtedly, the Post-Cold War military transformations driven by cyber technologies[11] have greatly extended the boundaries as to what is possible where it concerns the decision-making tempo.[12] The environment in which a military must operate has also changed dramatically, requiring a higher decision-making tempo to meet the challenges of a learning environment supercharged by cybernetic innovation. This of course includes the enemies one must face in this environment. Times have changed, and rapidly evolving information technologies have significantly increased the speed, agility, efficiency, and capacity of communication networks

(1) For an original battlespace knowledge work, see Libicki & Johnson, Dominant Battlespace Knowledge, 1996.

(2) See Mitchell (2012a, b, c, d, e,) where generic concept of agility is worked with specifically within the doctrinal context of warfighting.

(3) Mitchell (2012 d).

(4) See Mitchell (2012b) for tactical level examples from Helmand, Afghanistan, project Kitae.

(5) Cyber is a prefix that means "computer" or "computer network," as in cyberspace, the electronic medium in which online communication takes place. It includes the internet, telecommunications networks, computer systems, and embedded processors and controllers. (See US DoD Deputy Secretary of Defense Memorandum, dated 12 May 2008, defined cyberspace.) Cyber technology in this brief refers to wired, wireless, and optical technologies contributing to the convergence of computer and telecommunication networks in electromagnetic spectrums. Also see TRADOC Pam 525-7-8:15-18.

(6) See Boyd (1976).

(7) See Bares et al.(2010) for a detailed tactical example of how cyber is used to establish situational awareness.

(8) See Farrel et al. (2012) for conceptualization examples within the context of C2 and operational planning in the battlespace.

(9) Global Positioning System (GPS) Space-based satellite navigation system that provides location anywhere on or near the earth where there is an unobstructed line of sight to four or more GPS satellites.

(10) Some common 'off- the- shelve' examples include Skype, Facebook Chat, or Facetime.

(11) In Dostal (2003) the integration of Unmanned Aerial Vehicles (UAVs) and real-time video into the generation of situational awareness is discussed, it marks an extraordinary expansion observation capability for decision-making.

(12) See Alberts (2008) for an overview of transformation and information issues.

for everyone in (and around) the battlespace. Whether your organisation uses an expensive custom built encryption communication system that took 5 years to deploy or a truckload of 'off-the-shelf' mobile phones and 5 truckloads of prepaid SIM[13] cards that took 1 day to deploy, the resulting effect is a faster decision-making tempo. The availability of this technology also affects how we organise effectively on the back of cyber technologies. The traditional networked societies (those that did not go through industrialisation) have re-emerged stronger than ever, heralding their inherent organisational advantages in exploiting cyber driven communications.[14] The widespread use of cyber technology has created an extremely dynamic environment where maintaining/sustaining strategic advantage vis-à-vis an opponent is very difficult. Opponents simply have greater access to more information and thus learn faster than ever before. Properly exploited, cyber technologies can create OODA loops that appear to be metaphorically - on steroids. The real-time extraction of embedded map coordinates (GPS logged) from mobile phone pictures thrown up on social media such as Twitter in conflict, relayed automatically to waiting ISTAR[15] platforms, are case in point.

From a battlespace perspective, though the environment has become more dynamic, the two basic military premises noted by US Col. John Boyd, the developer of the OODA loop, still stand today: To defeat your enemy you must operate at a faster decision-making tempo than your adversary, or even better, get inside their decision-making process and mess it up through deception. [16] This brief will only deal with the issue of cybernetics versus the OODA *tempo*. The role of deception versus an adversary's OODA will be dealt with at another time. When assessing the OODA loop for tempo improvements due to cyber technologies, there must first be a general understanding of what 'improvement' entails for this brief.

'Improving' the Tempo?

When dealing with decision-making loops, improvement is directly related to the number of iterations[17] required to generate the desired effect and the total time of the total number of iterations required for generating the desired effect. For example, if *SYS X* takes 10 days and 20 iterations to generate the desired effect as compared to *SYS Y* that takes 5 days and 30 iterations, you could argue you get an improvement in time but not in quality. Real improvement would be to create a *SYS Z* that achieves the desired effects after 5 days in 20 iterations (See Fig. 1.0).Therefore, in principle, if technology is introduced that increases the speed of each iteration and reduces the number of iterations necessary to achieve the desired effect, one could certainly argue that there has been an improvement in terms of speed and precision. Moreover, improvements in speed and precision are improvements in agility.

(13) Subscriber Identification Module (SIM) is an integrated circuit that securely stores the international mobile subscriber identity (IMSI) and the related key used to identify the subscribers on mobile phones or computers. Having many prepaid SIM cards reduces the chances of the subscriber being discovered, identified, and located.

(14) For a good overview on how network organization has affected military thinking and planning, see the Joint War Fighting Centre's "*Commander's handbook for Attack the Network*".

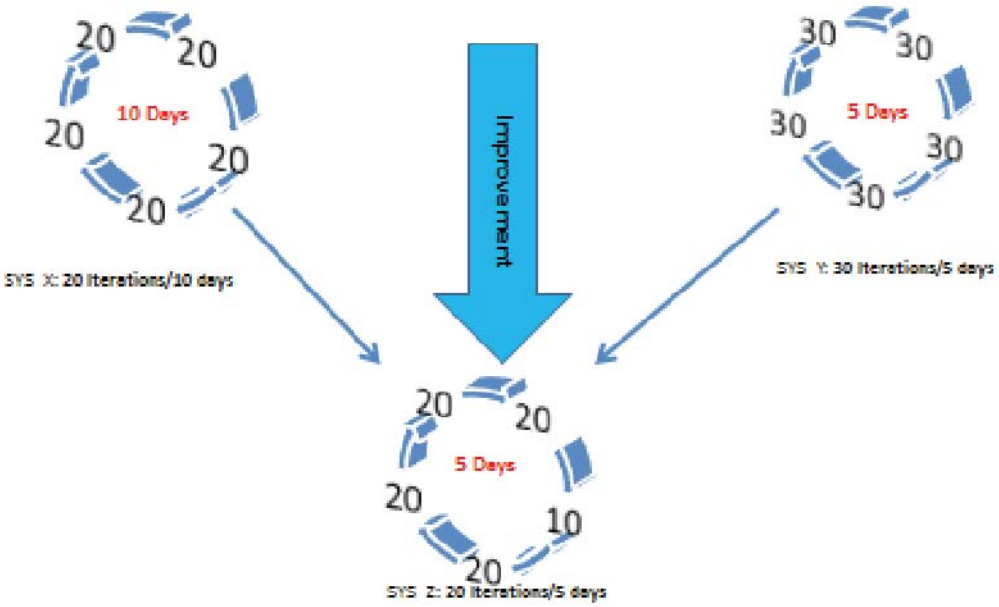
(15) ISTAR - Intelligence, Surveillance, Target Acquisition, and Reconnaissance

(16) See Boyd, John, R. (1995)

(17) *Iteration* refers to the act of repeating a process usually with the aim of approaching a desired goal, target, or result.

The above framework to assessment sounds more quantifiable than it actually is. As decision-making loops for organisations involve humans throughout, they are subject to the inherent cognitive complexities/inconsistencies of thinking men or women. Therefore where it concerns measurements of performance, observations placed within this framework remain squarely in the realm of qualitative observation and argumentation.

Fig.1.0 'Improving' the Tempo



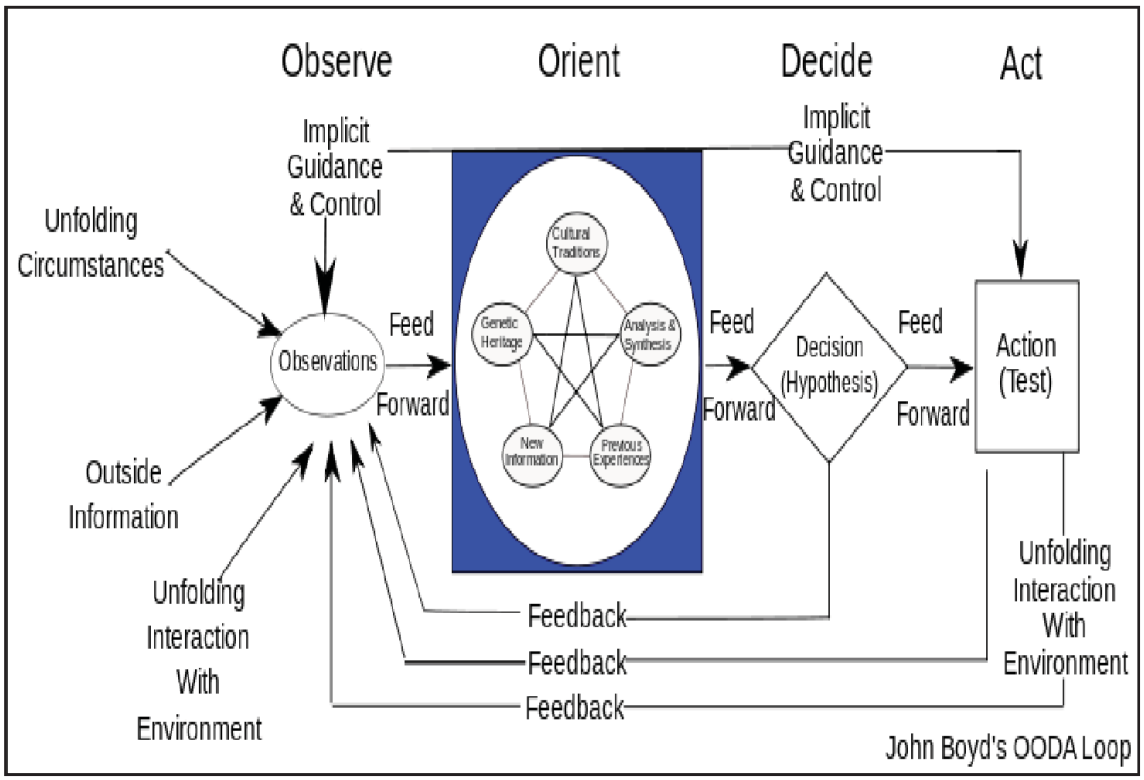
William Mitchell, Dept. of Joint Operations, Royal Danish Defence College, 2013

Cyber and the OODA Loop

The introduction of cyber technology to the OODA loop greatly increases the decision-making tempo with regards to both the number of iterations required and the time it takes to complete a single iteration. Looking at the Boyds' OODA loop starting from left to right, the *feed* or pre-cyber "*push*" principle can easily be identified as one progresses through the cycle from '*observations*' through '*analysis and synthesis'* and finally through to '*decision'* and '*action'* (See Fig. 2.0). It is here that current cyber driven technologies & software have their greatest effect on the decision-making tempo. This brief will only highlight three concepts, and the author hopes that a majority of readers should be able to relate to at least one of them. They

are MS SharePoint[18], JChat[19], and Clouding[20] which all by their very nature challenge the pre-cyber "*push*" principle by servicing the efficacy of a cyber-backboned "*pull*" principle.

Fig. 2.0 Observe- Orient- Decide-Act "LOOP"



Source: Wikimedia Commons, Patrick Edwin Moran 19 April 2008

The result is that the different stages of the loop no longer depend on calculating and communicating the needs of their required "*push*". Simply, all have real-time access to all stages of information management and take exactly what they need to resolve their issue, precisely

(18) Microsoft web application launched in 2001 based on Microsoft Office that allows for intranet portals, social networking, and document/file collaboration. It is the backbone of many "pull" systems as documents can be posted a one point that many actors in different locations can then work with. So instead of everyone sending emails with different versions of an attached report, all have access to the same version of a report on the SharePoint, even as it is generated.

(19) JChat is a joint command & control tool used by NATO as a communications network in a battlespace whereby chat rooms can be established to facilitate messaging communications traverse of the warfighting organisation. It also forms the backbone of '*tweeting*' information around the battlespace. It is extremely popular and also provides an automatic log of communications between commands for future reference. However some issues with regard to too many chat rooms being established in AFG - have been noted.

(20) *Clouding* refers to *cloud computing* whereby services are delivered to end user stations over a network and therefore reduce the use of local station resources (common examples are APPs for laptops or smartphones). Where it concerns warfighting, this has some advantages with regards to data storage, remote access, and interoperability. However it inherently has its own security issues.

when they need it. Metaphorically, the need to tell someone else what you need, and they go get it, or in a large hierarchal organization, that they in turn ask someone else to go get it for them, in order to give to you, is reduced. One obvious result then is a reduction in the number of 'return trip' communication filters between the original requesting unit and the knowledge source. This is extremely important where it concerns maintaining precision as 'context' is so essential to situational understanding. We know that 'context' inevitability succumbs to the erosion of accuracy through human interaction.[21] This cyber driven 'flat-lining' of communications also has an impact on speed. Both elements of the cyber contribution, increased speed and precision, should be captured in the following three vignettes that are used to characterise the movement from '*push*' to '*pull*'.

JChat

JChat refers to a chat communication network whereby anyone who has access to the chat rooms on the network[22] - can chat or post. It has been available for some time now (10 yrs +) and has been used in several different Theatres including Afghanistan (AFG). Essentially manoeuvre units in a battlespace can coordinate directly with each over JChat to resolve issues without requiring a higher HQ as a communication node. Furthermore, intelligence can be tweeted indiscriminately into the Theatre open chat forum as a post to be '*pulled*' off the network by the unit(s) which can use it.

1) *B Company tweets into the battlespace chat room that it has two units in contact at night and they could use some supporting flares - as they have used all of theirs. Without hesitation, D Company who is monitoring the chat immediately tweets an offer directly to B Company to fire flares in support of them. Noting no interjection 'tweet' from the Battle Group HQ fires staff over the chat, they immediately coordinate the supporting fires. D Company has essentially 'pulled' a mission off the network and self-synchronized its actions with B Company over the cyber driven chat network.*

2) *A U-2S Dragon Lady is flying over Theatre area at high altitude on a mission, when through passive signals collection; it incidentally picks up a reference to a possible IED being placed at a specific grid reference. The U-2S tweets a 1 liner into the Theatre wide JChat as follows: "U2 XYZ reporting possible IED at 32V MY 37600 97456." Dozens and dozens of tactical operational centres (TOCs) all across the Theatre read the tweet in the JChat, yet only the TOC with responsibility for the area around the actual grid reference pays any attention to it - and 'pulls' it off the chat network. The U-2S Dragon Lady never slows down from pursuing its main mission that has nothing to do with IEDs, and it will never know who, if anyone, far below – used the info. On the ground, a patrol is stopped by their TOC in its tracks meters from the IED, and precautions taken.*

(21) See Mitchell (2012a).

(22) Internet relay chat (IRC)

In this second example, all the stages of the OODA between the observation and the action are completed within seconds and include the side stepping of numerous formal organisational structures, command levels and geographical battlespace boundaries. Moreover, as illogical as a 'general' broadcast or tweet might sound when speaking of precision, there was almost picture precision in the delivery of the message from the source directly to the end user. This was accomplished not by traditional 'push' communications dynamic – but rather by the cyber driven 'pull' dynamic.

Clouding

Clouding allows all units (both lateral and vertical) across the organisation/order of battle/force laydown to access and '*pull*' down the data that is needed from a network. It also allows for greater data sharing support for extensive combined joint operations or comprehensive approaches that involve a wide variety of actors. The trick, in superficial terms, is to get the various databases and systems to feed into the same *cloud* that will act as the main resource for all actors involved and/or provide the main data management functions (like APPs.) Essentially, once an actor is plugged in, they can remotely access the data of all the actors involved that have made their data available.

> *For example, a special operations unit is conducting site exploitation of a suspected international terrorist base and is holding one suspect. With their remote/portable device, they scan the retinas and finger prints of the suspect and thereafter query a worldwide biometric database on terrorists via a satellite connection. They get lucky, as they score an ID hit on their suspect, and proceed to 'pull' down the file attached to the recognised fingerprints; the suspect is apparently wanted on the other side of the planet for making a car bomb upon which fingerprints matching his were found on a piece of the bomb's trigger mechanism by forensics specialists.*

In this example, cyber is providing historically unequalled remote access to very large amounts of data and analytical support, and doing so over great distances in a matter of minutes. Again, the cyber driven 'pull' principle is collapsing the inner time and space continuums (observe-orient-decide-act) of the OODA stages to extreme degrees. In this case, the OODA loop concerning the suspect's identification in terms of time, space, and precision.

SharePoint

The '*push*' principle has long been present in the traditional hierarchal military organisations. It is a method of disseminating knowledge to decision-makers vertically and horizontally across an organization by sending it through the right pipeline to get to the right user. Essentially, the use of SharePoints and Wiki type pages have contributed enormously to placing the onus of obtaining the knowledge on the end user, knowing where to go and get it. This in effect sums up the '*pull*' principle.

> *For example, across a coalition force of over 60,000, there are at least 5 command levels between Theatre level plans and the numerous tactical level framework opera-*

*tional units as well as 4 major geographical areas of command responsibility. Each day, like the many companies across Theatre, Company XYZ completes a report and posts it on their SharePoint (website.) At the very moment it is posted, several alerts are automatically triggered. They include several to its own battle group command (**2 levels up**), several to Brigade and Task Force, which incidentally have staff preparing reports on company XYZ's area for some larger operations (**4 levels up and 2 areas across**), and a LEGAD at the Theatre HQs reviewing a collateral damage related case (**5 levels up and 4 areas across.**) The alerts they established on Company XYZ' website tell them when something new is posted, so they can all visit Company XYZ's SharePoint and read or 'pull' the most recent report off the network. Company XYZ is busy planning next day's activities and is unaware of the totality of units or persons actually using their reports*.

These are just a few of the examples of a few cybernetic technologies that have severely impacted the tempo of the traditional OODA loop in Western militaries. There are obviously hundreds, if not thousands more, and new technologies are being produced every day. However, technology alone does not determine its own net-sum efficacy.

A 'Wee' Warning

It should be noted here with some understated vigour that tempo improvement is not just about what technology you use. It is also about the social and organisational context of *how* it is used. Though I am focusing on the technological advantages in this brief, I would like to present one vignette to illustrate the point that it is not all about what you have, but how you use it.

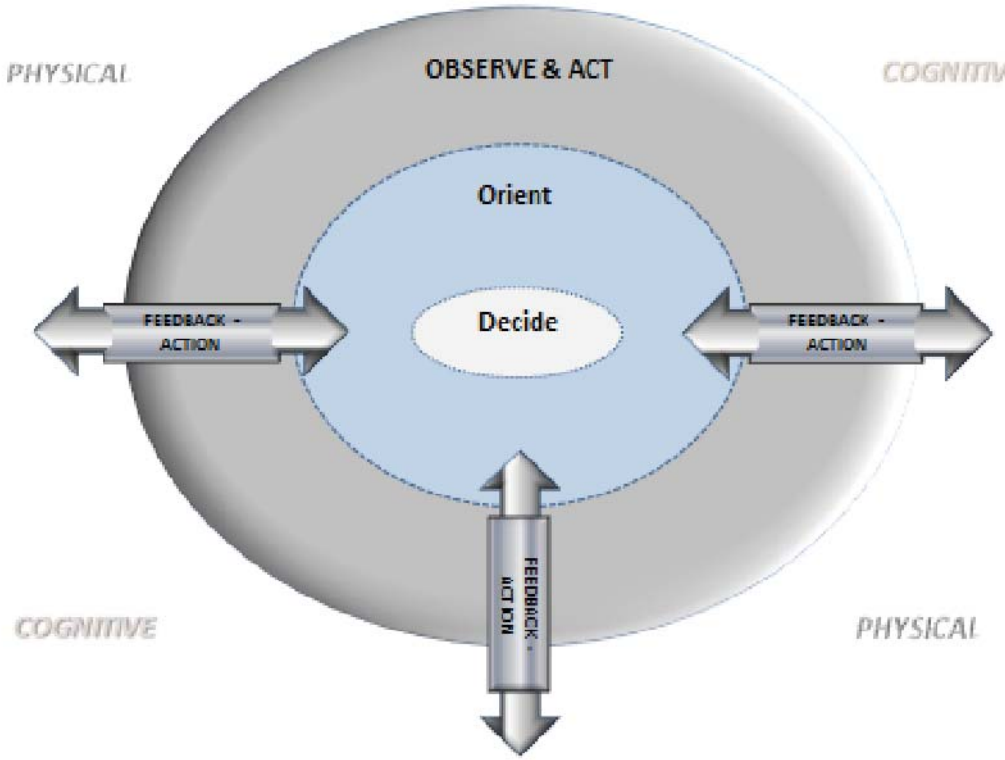
In the many cultures that did not experience industrialisations effects on social organisation, strong social networks driven primarily by blood relations remained intact to resolve problems. It should be of no surprise to anyone that when GSM/3G (mobile phone) networks became cheap and widespread, it greatly enhanced the range and speed of peoples who traditionally use network organisation. Nor can it be denied, that despite our technological advantages in the West, they are not always translated into a more efficient OODA loop. Ask the infantry radio operators slaving under the hot sun with kilos of batteries and kit. As they struggle to ensure communications between three different encrypted VHF nets over a distance of 30km to seek instructions from a Battalion HQ, while their opponent simply rings or sends an SMS to their boss directly for instructions – who happens to live 3000 km away.

The OODA "Moment"?

So what is the impact of cyber technologies on the OODA Loop? In the realities of today's cybernetic influence, not only does the Commander have real-time access to all information available horizontally and vertically within the structure of an organization. The different specialists, observers, sensors, collectors, analysts, planners, and those with authority to execute actions, also have immediate access. Thereby the different stages of Boyd's cycle become interwoven and synthesized in time and space through real time access and the emerging dominance of the '*pull*' principle. Due to the use of cybernetics, the central mechanism for *adaption,* the

OODA loop itself, is increasingly having a greater swath of its inner workings collapsed along a timeline that becomes shorter every day. Many aspects are already to a point where the human mind perceives that part of the process as being instantaneous. A good example is live UAV feed 10,000 km from the actual location of the UAV – in less than a second. So within the context of the OODA loop, cyber technologies offer opportunities to extremely reduce the time it takes to complete the iteration as well as reduce the total number of iterations necessary to achieve the desired effect. In fact, many aspects of the stages represented in the OODA loop now happen so quickly for the human mind that the staged process within the OODA loop resembles no more than momentary snapshots of feedback and actions perpetually passing each other on their way in and out of synthesized process (See Fig.3.0).

Fig.3.0 The OODA "Moment"



William Mitchell, Dept. of Joint Operations, Royal Danish Defence College, 2013

This in turn goes a long way in supporting battlespace agility as the exploitation of cybernetics significantly increases the speed of which knowledge is turned into actions for desired effects by the warfighting organisation. In many ways where once the collection and processing of information was the main time consumer within the OODA loop, the human factor in the form of authority to decide is itself becoming the greatest time consumer within OODA. Where once it was the lack of technology that was the greatest inhibitor to efficient decision-making within an organisation, today, it is likely the organisational structure that is the greatest obstacle to the efficient use of technology for faster decision-making.

Works Cited

Alberts, David S. *Information Age Transformation*. Washington D.C., US DoD CCRP, 2008.

Bares, Lt. Col. David et al. (2010) *A Tactical Framework for Cyberspace Situational Awareness*. 15th ICCRTS Evolution of C2, June 22-24, Santa Monica, California

Boyd, John, R., The Essence of Winning and Losing, 28 June 1995 a five slide set by Boyd

Boyd, John, R., Destruction and Creation. US Army Command and General Staff College, September 3, 1976

Dostal, B.C. (2007). Enhancing situational understanding through the employment of unmanned aerial vehicles. Army Transformation Taking Shape ...Interim Brigade Combat Team Newsletter, No. 01–18. Retrieved November 7, 2007, from http://www.globalsecurity.org/military/library/report/call/call_01-18_ch6.htm

Edison, Tom. (2005) 'Social Networking Analysis: One of the First Steps in Net-Centric Operations' *Defense Acquisition Review Journal*, Alexandria 2005: 294-303.

Farrel, Robert J. Jr. et al. Cornerstone: Foundational Models and Services for Integrated Battle Planning. 17th ICCRTS Operationalizing C2 Agility, June 17-21, 2012,Washington D.C. pp.3-4

Joint Warfighting Centre, Commander's handbook for Attack the Network, Version 1.0: United States Joint Forces Command, 2011

Libicki, Martin C. and Stuart E. Johnson, eds. (1996) "Dominant Battlespace Knowledge". April 1996.

Mitchell, William. (2012a) *Kitae I: Battlespace Agility in Helmand: Network vs. Hierarchy C2*. (Copenhagen: Royal Danish Defence College Press, 2012) http://forsvaret.dk/FAK/PUBLIKATIONER/RESEARCH%20PAPERS/Pages/Forsvarsakedemiet%20Working%20Papers.aspx#publication_b1399452-e6dd-4abb-b2e0-98633d9c089f

Mitchell, William. (2012b) *Kitae II: Battlespace Intelligence: Social Network vs. Traditional Time & Space Analysis in Helmand* (Copenhagen: Royal Danish Defence College Press, 2011) http://forsvaret.dk/FAK/PUBLIKATIONER/RESEARCH%20PAPERS/Pages/Forsvarsakedemiet%20Working%20Papers.aspx#publication_b1399452-e6dd-4abb-b2e0-98633d9c089f

Mitchell, William. (2012c) *Three C2 Models for Military Agility in the 21st Century*. (Copenhagen: Royal Danish Defence College Press, 2012) http://forsvaret.dk/FAK/PUBLIKATIONER/BRIEFS/Pages/Forsvarsakademiet%20Briefs.aspx#publication_f9c8df66-4093-4072-9a08-20398ce7c2a7

Mitchell, William. (2012d) *Battlespace Agility 101: The Use of Target Network Modelling to Increase Shared Situational Awareness and Understanding* (Copenhagen: Royal Danish Defence

College Press, 2012) http://forsvaret.dk/FAK/PUBLIKATIONER/BRIEFS/Pages/Forsvarsakademiet%20Briefs.aspx#publication_bb74761b-58af-44b8-934c-27a21d74383e

Mitchell, William(2010b). Agile Sense-Making in an Intersubjective Environment. *International C2 Journal* (IC2J). Spring 2010.
http://www.dodccrp.org/html4/journal_v4nl.html

NATO SAS-085 (Forthcoming 2013) Operationalizing Agility

NATO (2002) Code of Best Practice of C2 Assessment Analysts Summary Guide, Washington: CCRP

Phister, Paul W. Jr. Humans and Their Impact on Cyber Agility. 17th ICCRTS Operationalizing C2 Agility, June 17-21, Washington D.C. pp. 18.

Phister, Paul W. Jr., Timothy Busch, & Igor G. Plonisch, (2004) Joint Synthetic Battlespace: Cornderstone for Predictive Battlespace Awareness., Rome, NY: Air Force Research Laboratory/Information Directorate, 2004

SAB-TR-02-01, "Predictive Battlespace Awareness to Improve Military Effectiveness, Air Force Scientific Advisory Board, August, 2002.

Schoffner, Wilson A. (1993) "Future Battlefield Dynamics and Complexities Require Timely and Relevant Information", Phalanx, 26(1). 1993, 31-35

United States Army, TRADOC 525-7-8, Cyberspace Operations Concept Capability Plan 2016-2028, 22 February 2010.