Modern Militaries and a Network Centric Warfare Approach

https://www.e-ir.info/2014/01/09/modern-militaries-and-a-network-centric-warfare-approach/

JONJO ROBB, JAN 9 2014

To What Extent Do Modern Military Operations Require a Network Centric Warfare Approach?

Throughout the twentieth century, advancements in technology have coincided with significant developments in the way militaries of the world wage combat. From the use of cavalry units at the outbreak of the First World War to the deployment of Unmanned Aerial Vehicles in *Operation Allied Force,* technology has allowed the way in which military operations are conducted to evolve considerably. As we look into the twenty-first century, technology continues to play a greater role in the way these militaries operate. However, it is not simply new weapons, aircraft or warships that are transforming the militaries of today. The way in which forces communicate, disseminate intelligence, are issued orders, and report back to their commanders has been revolutionised through the use of networks. More specifically, computer, radio and data networks link nearly all military assets at a state's disposal to each other and to the decision makers. From the nuclear ballistic missile submarines lurking under the oceans to the commanders on the ground in Afghanistan, the doctrine of network centric warfare gives a military the ability to 'to attain a high level of shared battlespace awareness that is exploited to achieve strategic, operational, and tactical objectives in accordance with the commander's intent.'[1] This includes not just joint warfare in a specific theatre of operations, but also the coordination of dispersed forces on a global level.

There are various definitions of the term Network Centric Warfare (NCW), although all agree that NCW's basic tenet is the use of networked technology to provide an advantage on the battlefield. A US Congressional Research Service report defines network-centric operations (NCO being a term used interchangeably with NCW) as operations that rely 'on computer equipment and networked communications technology to provide a shared awareness of the battle space for U.S. forces'.[2] Other nations may refer to the concept differently; the United Kingdom, for example, denotes this as Network Enabled Capability.[3] In the following paper, the case will be made that to enhance a military's war-fighting capability and to increase the likelihood of success in operations, a network-centric approach to military operations is paramount.

What Network Centric Warfare Brings to the Battlefield

We are presently living in an era defined by many as the 'information age'. Technology is all around us and in one form or another related to everything we do, with warfare being no different. Some describe the increasing role that technology plays in war as a 'technical revolution in military affairs that is changing the nature of war fighting and security operations'.[4] Whether or not it is justifiable to regard this as a revolution in military affairs, it is at least widely agreed that technology is rapidly changing the way military objectives are accomplished. NCW is therefore an increasingly necessary theory of war to ensure that critical information gets to those who need it fast, whether it is those on the battlefield or those making the decisions at HQ. David S. Alberts, who formerly worked in the office of the Assistant Secretary of Defense for Networks and Information Integration, lists the four foundational advantages of NCW to be:

1. A robustly networked force improves information sharing.
2. Information sharing and collaboration enhance the quality of information and shared situational awareness.

3. Shared situational awareness enables self-synchronization.
4. These, in turn, dramatically increase mission effectiveness.[5]

Obviously, any method of conducting operations that is expected to increase mission effectiveness will be welcomed by any armed forces. The US Department of Defense goes as far to say that 'Forces that are networked outfight forces that are not, everything else being equal.'[6] The document also makes the claim those only military forces that are 'truly joint, with comprehensively integrated capabilities and operating according to the principles of NCW, can fully exploit the highly path-dependent nature of Information Age warfare.'[7] This certainly enforces the view that modern military operations require a network-centric approach to be effective. Of course, the chances of a military facing an almost-symmetric opponent with the only difference between them being one side conforming to the NCW doctrine is extremely rare, so the validity of the first statement is certainly questionable. Nonetheless, it is indubitable that possessing an NCW capability does indeed prove to be a 'game changer' when facing an enemy who does not possess such capability.

Another key advantage of the NCW doctrine is the ability for Command & Control (C2) of forces spread over a large geographical area (perhaps in different theatres) in a more expeditious and efficient manner. Networks 'harness the power of geographically dispersed nodes by linking them together into networks that allow for the extremely rapid, high-volume transmission of digitized data.'[8] The ability to disseminate instructions, information and intelligence to assets dispersed across the globe is particularly vital for those forces which are likely to be involved in expeditionary warfare, such as those of the United States and to a lesser extent the United Kingdom, who at present have a global reach.

Network Centric Warfare in Action

Having previously described the reasons why NCW is an integral part of modern military operations, this essay will now demonstrate how NCW doctrine has been applied in practical situations. The US-led invasion of Afghanistan in 2001 provides just one of many examples of the successful deployment of the NCW theory of war. Jeffrey L. Groh describes how during *Operation Enduring Freedom* Special Forces on the ground were able to use data and voice links provided by communication satellites to co-ordinate their efforts. Not only were the ground forces able to communicate with each other, but also with F-14's, F-15E's, B-1 and B-2 aircraft by laser designating targets that the air support would later destroy with Joint Direct Attack Munitions (JDAM).[9] JDAM-equipped 'smart munitions' are guided to their targets by an inertial guidance system and the global positioning system (GPS), once again making use of space-based technologies. Further to this Colonel Harry Tunnell, who was Commander of Task Force Stryker in Afghanistan, has written about how valuable NCW was on the battlefield. Tunnell's task force used*ASCOPE1 Decision Maker,* 'an ArcGIS-based tool that provides geospatial representation of multiple layers of specific information'[10] as well as the *Battle Command Visualization Suite* which 'fuses intelligence; operations; geospatial data; and governance, reconstruction, and development information for display on Google Earth.'[11] Tunnell concluded that NCW enhanced operations and developed 'rapid, effective situational understanding. True network-centric operations are far more than merely improved situational awareness—they include a level of understanding that can only be gained through disciplined research and analysis.'[12]

Moving away from surface warfare, another example of NCW's success in operations is *Link 16*, and the advantage it gives to the air forces that make use of it. *Link 16*, also known as TADIL-J (Tactical Digital Information Link J) is described as a 'communication, navigation, and identification system that supports information exchange between tactical command, control, communications, computers, and intelligence (C4I) systems.'[13] The system uses encrypted messages and transmissions which are jam resistant to provide the user with a whole host of possible applications. These include surveillance, electronic warfare, mission management/weapons coordination, air control, positive friendly identification and network management.[14] The RAND Corporation's National Defense Research Institute (NDRI) conducted a case study to determine the impact of using *Link 16* in an air-to-air combat situation. NDRI summarised their findings by stating that when *Link 16* was used 'the quality of information available to individual fighter pilots was increased significantly'[15] and that pilots 'were on average able to make better decisions and make decisions earlier in the opening gambits of tactical air-to-air engagements. This resulted in greatly increased force effectiveness.'[16] *Link 16,* combined with the Eurofighter Typhoon's long range radar provided

pilots with 'exceptional and unrivalled situational awareness of the operating area'[17] during *Operation ELLAMY* over Libya in 2011. The system has also seen operational use over Bosnia, Iraq and Afghanistan.[18]

Drawbacks of Network Centric Warfare

Thus far, both the theoretical concepts surrounding NCW and the practical uses of the doctrine have been described. This paper has clearly demonstrated with ample evidence from recent military operations that in the increasingly technological theatre of war a network centric approach to modern military operations in indispensable for achieving information dominance and an upper hand over any potential adversary. Although this essay demonstrates how Network Centric Warfare is an integral component of modern conflict, NCW is not without its deficiencies. It is important to address these issues so as to give a fuller insight into the NCW concept. One of the major issues identified with NCW is a heavy reliance on technology, particularly infrastructure. There are various reasons why reliance on infrastructure brings with it significant risk. It can become the 'primary centre of gravity for opponents to exploit'.[19] This is particularly hazardous if alternative ways of working are not available.[20] If NCW becomes so critical to warfare that forces become incapable of fighting in a non-network centric fashion, there is little doubt that any disruption to networks that they are dependent on could be catastrophic and potentially crippling for a military. Nor is there any doubt that a capable enemy would attempt to exploit this weakness by disrupting networks. A case in point would be the proliferation of GPS jammers. The Commander of United States Air Force Space Command has identified that US forces have 'a very heavy reliance on space and we consider GPS foundational in military operations'.[21] Indeed, GPS has been described as 'the core asset required for NCW to work'.[22] However, in recent years GPS jammers which can block GPS signals have become more widely available than ever before. If a jammer is used by an enemy it has the potential to 'eliminate GPS navigation and precision guidance capabilities within an extensive area of operations'.[23] Quite clearly, a loss of GPS capability would have calamitous effects on the US' war fighting capability, as would be the case with the majority of the world's armed forces that utilise the GPS system. This would be mostly damaging for those forces relying on network-centric navigational systems, to which GPS is a major component.

Conclusions

This essay has demonstrated that Network Centric Warfare has been established as a core element of modern military operations. Given the ever-evolving and increasing role that technology possesses in warfare, NCW becomes more crucial to make certain that forces have the information, intelligence and situational awareness they require to achieve their objectives. Not only is technology changing conflict, but the manner in which militaries wage war is also changing. An increasingly prevalent theory of war is that of joint operations, defined by the US Department of Defense as 'military actions conducted by joint forces and those Service forces in specified command relationships with each other'.[24] As armies, air forces and navies work together to achieve political goals, warfare becomes more complex and operations become larger. Carl von Clausewitz talks of the uncertainty of information that is experienced in the fog of war.[25] Although this paper does not suggest that NCW can lift this fog totally, the evidence suggests that NCW brings a degree of clarity and awareness to the battlefield. Using communications technology to provide even dispersed forces with the latest information guarantees that forces are better informed and therefore more likely to make the right decisions. Successful joint operations depend on a number of very different but capable forces working together. A centralised C4ISTAR[26] infrastructure as part of the NCW doctrine can oversee such joint operations and act as a hub for communication with and direction of any of the units in the theatre, be it a Tornado GR4 or a team of Special Forces. To summarise, NCW is an 'integration of sensors, decision-makers, weapons platforms and support capabilities to enable agility'[27] providing 'interoperability and collaboration within and between services'.[28]

NCW provides a level of situational awareness that allows the military to be more flexible, which without doubt increases mission effectiveness. However, it is clear that NCW is not by any means without flaws. A heavy reliance on technology is problematic, as it cannot be ruled out that technology may fail, may not be available at the time, or as discussed earlier, may be targeted by an enemy to reduce war-fighting capability. As NCW becomes more predominant, steps must be taken to safeguard it from malicious action. It is also imperative that forces can operate in a fall back mode without the NCW doctrine, if required of them. Assuming that these vulnerabilities can be

addressed, it has been shown in this essay that Network Centric Warfare is an essential element of modern military operations. It is increasingly relevant to conduct warfare in such a manner that, as a force multiplier, considerably increases a military's ability to be successful in a wide range of operations.

Bibliography

Air Land Sea Application Center, Introduction to Tactical Digital Information Link J and Quick Reference Guide. Available from: http://www.globalsecurity.org/military/library/policy/army/fm/6-24-8/tadilj.pdf [Accessed 14 November 2013].

Alberts, D., 'Information Age Transformation: Getting to a 21st Century Military' (Washington, DC: Department of Defense Command and Control Research Program, 2002).

Alterman, S., Information Assurance: Trends in Vulnerabilities, Threats, and Technologies (Memphis, General Books, 2011).

Center for Technology and National Security Policy, 'Task Force Stryker Network-Centric Operations in Afghanistan' (Washington DC: National Defense University, 2011).

Clausewitz, C., On War (Oxford, Oxford University Press, 2008).

Congressional Research Service, 'Network Centric Operations: Background and Oversight Issues for Congress' (Washington DC: Congressional Research Service, 2007).

CQ Roll Call, The Pentagon's GPS Problem. Available from: http://public.cq.com/docs/weeklyreport/weeklyreport-000004218242.html [Accessed 14 November 2013].

Defence Scientific and Technical Laboratory (Dstl) and QinetiQ plc, Potential System Vulnerabilities of a Network Enabled Force. Available from: http://www.dodccrp.org/events/9th_ICCRTS/CD/papers/131.pdf [Accessed 14 November 2013].

Dombrowski, P., Gholz, E. and Ross, A., Military Transformation and the Defense Industry after Next: The Defense Industrial Implications of Network-Centric Warfare (Newport, United States Naval War College, 2003).

Gonzales, D., Hollywood, J., Kingston, G. and Signori, D., Network-centric operations case study: air-to-air combat with and without Link 16 (Santa Monica, RAND Corporation, 2005).

House of Commons Defence Select Committee, Letter from Peter Luff MP, Minister for Defence Equipment, Support and Technology, Ministry of Defence. Available from: http://www.publications.parliament.uk/pa/cm201012/cmselect/cmdfence/950/950we06.htm [Accessed 14 November 2013].

Ministry of Defence Joint Service Publication 777 Edn 1, 'Network Enabled Capability' (London: Ministry of Defence UK, 2005).

Ministry of Defence 'Understanding Network Enabled Capability' (London: Newsdesk Communications Ltd, 2009).

Office of Force Transformation, United States Department of Defense, 'The Implementation of Network-Centric Warfare' (Washington DC: US Government Printing Office, 2005).

Office of Force Transformation, United States Department of Defense, 'The Implementation of Network-Centric Warfare Brochure' (Washington DC: US Government Printing Office, 2005).

Thales UK, Link 16 Operational Overview. Available from: https://www.thalesgroup.com/sites/default/files/asset/document/White%20Paper%20-%20Link%2016%20Overview.pdf [Accessed 14 November 2013].

United State Department of Defense, 'Joint Publication 1: Doctrine for the Armed Forces of the United States' (Washington DC: US Government Printing Office, 2013).

USAWC Guide to National Security Issues, Vol I: Theory of War and Strategy, 'Network-Centric Warfare: Leveraging the Power of Information' (Carlisle: Strategic Studies Institute of the US Army War College, 2008).

[1] Office of Force Transformation, United States Department of Defense, 'The Implementation of Network-Centric Warfare' (Washington DC: US Government Printing Office, 2005), p. i.

[2] Congressional Research Service, 'Network Centric Operations: Background and Oversight Issues for Congress' (Washington DC: Congressional Research Service, 2007), Summary.

[3] Ministry of Defence Joint Service Publication 777 Edn 1, 'Network Enabled Capability' (London: Ministry of Defence UK, 2005).

[4] Ministry of Defence 'Understanding Network Enabled Capability' (London: Newsdesk Communications Ltd, 2009), p. 12.

[5] Alberts, D., 'Information Age Transformation: Getting to a 21st Century Military' (Washington, DC: Department of Defense Command and Control Research Program, 2002), p. 7.

[6] Office of Force Transformation, United States Department of Defense, 'The Implementation of Network-Centric Warfare Brochure' (Washington DC: US Government Printing Office, 2005)

[7] *Ibid*

[8] Dombrowski, P., Gholz, E. and Ross, A., Military Transformation and the Defense Industry after Next: The Defense Industrial Implications of Network-Centric Warfare (Newport, United States Naval War College, 2003), p. 6.

[9] USAWC Guide to National Security Issues, Vol I: Theory of War and Strategy, 'Network-Centric Warfare: Leveraging the Power of Information' (Carlisle: Strategic Studies Institute of the US Army War College, 2008), p .325.

[10] Center for Technology and National Security Policy, 'Task Force Stryker Network-Centric Operations in Afghanistan' (Washington DC: National Defense University, 2011), p. 1.

[11] *Ibid*

[12] Center for Technology and National Security Policy, 'Task Force Stryker Network-Centric Operations in Afghanistan' (Washington DC: National Defense University, 2011), p. 17.

[13] Air Land Sea Application Center, *Introduction to Tactical Digital Information Link J and Quick Reference Guide.* Available from: http://www.globalsecurity.org/military/library/policy/army/fm/6-24-8/tadilj.pdf [Accessed 14 November 2013]. P. I-1.

[14] Air Land Sea Application Center, *Introduction to Tactical Digital Information Link J and Quick Reference Guide.* Available from: http://www.globalsecurity.org/military/library/policy/army/fm/6-24-8/tadilj.pdf [Accessed 14 November 2013]. P. I-2.

[15] Gonzales, D., Hollywood, J., Kingston, G. and Signori, D., Network-centric operations case study: air-to-air combat with and without Link 16 (Santa Monica, RAND Corporation, 2005), p. 75.

[16] *Ibid*

[17] House of Commons Defence Select Committee, *Letter from Peter Luff MP, Minister for Defence Equipment, Support and Technology, Ministry of Defence.* Available from: http://www.publications.parliament.uk/pa/cm201012/cmselect/cmdfence/950/950we06.htm [Accessed 14 November 2013].

[18] Thales UK, *Link 16 Operational Overview.* Available from: https://www.thalesgroup.com/sites/default/files/asset/document/White%20Paper%20-%20Link%2016%20Overview.pdf [Accessed 14 November 2013]. p. 1.

[19] Defence Scientific and Technical Laboratory (Dstl) and QinetiQ plc, *Potential System Vulnerabilities*

of a Network Enabled Force. Available from: http://www.dodccrp.org/events/9th_ICCRTS/CD/papers/131.pdf [Accessed 14 November 2013]. p .15.

[20] *Ibid*

[21] CQ Roll Call, *The Pentagon's GPS Problem.* Available from: http://public.cq.com/docs/weeklyreport/weeklyreport-000004218242.html [Accessed 14 November 2013].

[22] Alterman, S., Information Assurance: Trends in Vulnerabilities, Threats, and Technologies (Memphis, General Books, 2011), p. 134.

[23] *Ibid*

[24] United State Department of Defense, 'Joint Publication 1: Doctrine for the Armed Forces of the United States' (Washington DC: US Government Printing Office, 2013), p. xi.

[25] Clausewitz, C., On War (Oxford, Oxford University Press, 2008), p. 88.

[26] Command, control, communications, computers, intelligence, surveillance, target acquisition, and reconnaissance

[27] Ministry of Defence Joint Service Publication 777 Edn 1, 'Network Enabled Capability' (London: Ministry of Defence UK, 2005).

[28] *Ibid*

—

Written by: Jonjo Robb
Written at: Aberystwyth University
Written for: Dr. Kristan Stoddart
Date written: November 2013