

Canadian
Forces
College

Collège
des
Forces
Canadiennes



DISTRACTED WARFIGHTERS: PITFALLS OF THE DIGITAL BATTLEFIELD

MAJOR TOM MCMULLEN

JCSP 46

Service Paper

Disclaimer

Opinions expressed remain those of the author and do not represent Department of National Defence or Canadian Forces policy. This paper may not be used without written permission.

© 2020 Her Majesty the Queen in Right of Canada,
as represented by the Minister of National Defence.

PCEMI 46

Étude militaire

Avertissement

Les opinions exprimées n'engagent que leurs auteurs et ne reflètent aucunement des politiques du Ministère de la Défense nationale ou des Forces canadiennes. Ce papier ne peut être reproduit sans autorisation écrite.

© 2020 Sa Majesté la Reine du Chef du Canada,
représentée par le ministre de la Défense nationale.

CANADIAN FORCES COLLEGE – COLLÈGE DES FORCES CANADIENNES

JCSP 46 – PCEMI 46
2019 – 2020

SERVICE PAPER - ÉTUDE MILITAIRE

DISTRACTED WARFIGHTERS: PITFALLS OF THE DIGITAL BATTLEFIELD

Major Tom McMullen

“This paper was written by a candidate attending the Canadian Forces College in fulfillment of one of the requirements of the Course of Studies. The paper is a scholastic document, and thus contains facts and opinions which the author alone considered appropriate and correct for the subject. It does not necessarily reflect the policy or the opinion of any agency, including the Government of Canada and the Canadian Department of National Defence. This paper may not be released, quoted or copied, except with the express permission of the Canadian Department of National Defence.”

Word Count: 2,429

« La présente étude a été rédigée par un stagiaire du Collège des Forces canadiennes pour satisfaire à l'une des exigences du cours. L'étude est un document qui se rapporte au cours et contient donc des faits et des opinions que seul l'auteur considère appropriés et convenables au sujet. Elle ne reflète pas nécessairement la politique ou l'opinion d'un organisme quelconque, y compris le gouvernement du Canada et le ministère de la Défense nationale du Canada. Il est défendu de diffuser, de citer ou de reproduire cette étude sans la permission expresse du ministère de la Défense nationale. »

Nombre de mots : 2.429

DISTRACTED WARFIGHTERS: PITFALLS OF THE DIGITAL BATTLEFIELD

AIM

1. This service paper considers the perils related to the increasing digitization of the battlefield, specifically with respect to the ongoing efforts to connect front-line warfighters to high-speed networked information systems enabled by modern communications technology. The purpose of the paper is to highlight these pitfalls while also recommending best practices to mitigate their risks.

INTRODUCTION

2. Ongoing improvements in modern communications technology has largely resolved the challenge of connecting commanders, sensors, and shooters throughout the digital battlefield for the purported benefits of improved shared awareness, heightened operational tempo, and better informed decision-making. But efforts to push networked systems down to the warfighter level introduce harmful side effects which commanders must appreciate. This paper illustrates that the desire to achieve interconnectivity between warfighters to exploit the perceived advantages of the digital battlefield may actually have detrimental effects on decision-making if not properly understood and managed.

3. The paper first reviews the dangers of operator information overload wherein warfighters spend the majority of their time processing information rather than completing their tasks. The paper then considers how instantaneous digital communication across the battlefield can lead to counter-productive information appetites; promotes centralisation of authority; and amplifies the spread of misinformation. Finally, the paper looks at the vulnerability introduced by western

militaries' overconfidence in uninterrupted communications across the digital battlefield which are sure to fail or be denied in combat. Throughout the discussion, the paper offers best practices which should be considered by commanders to mitigate against these pitfalls. The paper concludes by offering general recommendations on this topic.

DISCUSSION

4. One of the consequences of increased information distribution across the battlefield is the impact on the attention of warfighters. Soldiers who are expected to perform their primary tasks of *shoot, move, communicate*, must now be ready to deal with more frequent interruptions and attention-grabbing context switches generated by modern communications and soldier systems (e.g., personal communication devices networked to sensors and information databases). Human factors research demonstrates that individuals cannot perform two information-processing tasks as quickly as one.¹ Although training may improve multi-tasking abilities—e.g., experienced armoured crew commanders can visually monitor their surroundings during travel while also exchanging information over radio nets—the increase in information processing demands from soldier systems, often through visual cues, can dangerously distract from their essential tasks. For example, information overload was blamed when a US Air Force drone operator, in February 2010, failed to observe the forming of an Afghani civilian (including children) convoy, which was tragically fired upon by US strike helicopters.² The operator was distracted by

¹ Martin, John, Laurel Allender, Pamela Savage-Knepshield, and John Lockett, eds. *Designing Soldier Systems: Current Issues in Human Factors* (CRC Press, 2018), 72.

² Shanker, Thom, and Richtel, Matt. "In New Military, Data Overload Can Be Deadly." *The New York Times*, January 16, 2011. Accessed 24 October, 2019.
<https://www.nytimes.com/2011/01/17/technology/17brain.html>

multiple cognitive tasks—numerous instant messaging windows with intelligence analysts and ongoing voice communications with troops on the ground over radio—and failed to adequately concentrate on his essential task of observing the drone’s video surveillance feed overlooking the convoy.

5. Connected warfighters may also be expected to search through networked data stores to find relevant information and intelligence to support their decision-making. Such information may be difficult to find (e.g., searching through multiple data stores) while also necessitating confirmation of information accuracy and authenticity. This results in skilled operators collecting and tracking data—i.e., fighting the system—rather than performing their essential tasks.

6. Commanders must also appreciate the limits of their soldiers’ information processing capacity which is often determined by how much the senior end can transmit rather than how much the junior end can conveniently assimilate.³ Moreover, soldiers must also determine which incoming signals are important from the noise and decide if newly received information may change their mission or affect their tasks. For example, during the Falklands War, Admiral Sandy Woodward, Commander of the deployed British Maritime Task Group, required dedicated operations staff on his flagship to process over five hundred daily signals from his higher headquarters in Northwood, UK.⁴

7. Information prioritisation mechanisms can also become dislocated in times of overload. For example, when fighting in the Gulf War began in January 1991, a backlog

³ Gordon, Andrew. *The Rules of the Game: Jutland and British Naval Command* (Naval Institute Press, 2013), 584.

⁴ Woodward, Sandy, and Patrick Robinson. *One Hundred Days* (London: HarperPress, 2012), 157

of signals sent to the deployed UK naval task force led to “‘Routine’ messages being competitively upgraded to ‘Priority’, ‘Priority’ to ‘Immediate’, ‘Immediate’ to ‘Flash’ and so on as the congestion shifted upwards”.⁵

8. Although the push of digital communications to lower levels and improvements to soldier systems are certainly advantageous, commanders must understand and appreciate their drawbacks and must be prepared to enforce strict self-denying discipline from themselves and their staff to avoid contributing to information overload. At their end, operators would do well to avoid becoming servants to the technologies and consider assigning dedicated information processing tasks to members of their outfit to reduce distractions from their tasks. For instance, subunits in the field may consider employing data clerks whose primary function would be to filter data and draft correspondence to unburden fellow warfighters from this tedious work. Research has also shown that soldier systems employing tactile feedback⁶ tends to enhance soldier performance and lowers cognitive workload by reducing visual and auditory signals so they may be directed towards their essential tasks (e.g., soldiers on patrol in a village in a counter-insurgency context who must prioritise visual and auditory cues to observe and react to changing situations).

9. The paper now moves to discuss how the seduction of instantaneous digital communications across the battlefield introduces three main challenges. First, commanders and headquarters staff may develop insatiable information appetites through the exponential increase of connected battlefield sensors and fueled by their desire to

⁵ Gordon, *The Rules of the Game...*, 585

⁶ Martin, *Designing Soldier Systems...*, 85

strive for near-perfect intelligence in support of their decisions. But more information does not necessarily equate to better intelligence; rather it introduces a heavier burden on information analysts who must sift through reams of collected data to draw out actionable intelligence, effectively slowing down overall decision making and tempo. This was observed during the 1991 Gulf War and was coined the ‘Schwarzkopf syndrome’ by Ferris and Handel⁷ wherein commanders demonstrated the “desire to wait just one more moment...to read just one more report, the reluctance to act on imperfect knowledge because it is known to be imperfect and that at any point another report might well produce perfection.” As Ferris and Handel discuss, Clausewitz offers practical advice to commanders who contend with intelligence uncertainty: “to ignore intelligence and to act exclusively on informed intuition, because only through these means can commanders hope to deal with the world.”⁸ No doubt that modern-day commanders would be hard-pressed to follow such advice.

10. Second, commanders must guard against overcontrol and centralisation of authority promoted by the power of instantaneous communications. As retired US Secretary of Defence and Marine Corps General Jim Mattis warns, “digital technology— instant questions demanding instant responses—conveys to higher headquarters a sense of omniscience, an inclination to fine-tune every detail below.”⁹ When such tight communications control is imposed by commanders, it leads to what Mattis terms

⁷ Ferris, John, and Michael I. Handel. “Clausewitz, Intelligence, Uncertainty and the Art of Command in military operations.” *Intelligence and National Security* 10, no. 1 (1995): 50

⁸ *Ibid.*

⁹ Mattis, Jim, and West, Bing. *Call Sign Chaos: Learning to Lead* (New York: Random House, 2019), 43

“Mother, may I’ timidity” from subordinate commanders and causes hesitation and loss of initiative. This was observed during the early stages of the Falklands War where the overall Task Force Commander, Admiral John Fieldhouse, acted as commander of all forces deployed in the Falklands area of operations, more than 8000 miles from his Headquarters in Northwood, UK, facilitated by satellite communications links to his subordinate commanders.¹⁰ Subordinates, sensing such overcontrol and centralisation of command, are advised to break free from these bonds and make clear to their superiors how such systems can suffocate initiative. Returning to the Falklands War example, Admiral Woodward, on-site commander in the Falklands, sent an attack order to one of the British submarines (not under his command) knowing full well that such an order would be intercepted and removed by his superior, Admiral Fieldhouse, in the UK, but which had the requisite effect of signaling the need for a change in the command relationship.¹¹

11. Third, instant communications also instantly amplify misinformation which will spread throughout the network contributing to thickening the fog of war (ironically that which was advertised as having been eliminated by the promise of network-centric warfare). Commanders, their staffs, and warfighters at all levels must ensure they vet the information they receive and trust that data they use in their decision calculus is both accurate and credible. Not only are decision-makers vulnerable to disinformation (e.g., cyber attacks which may alter sensor data such as GPS coordinates), but they must also seek to contain the spread of erroneous reporting which is normal with early reports in

¹⁰ Gordon, *The Rules of the Game...*, 586

¹¹ *Ibid.*, 587

developing situations where commanders may perceive the same information in different ways. This problem can be mitigated by headquarters close-holding first reports—if the communication system allows it—at their level until clarity is achieved. Commanders are also encouraged to maximise use of face-to-face (or voice over telephone) conversations where “both meaning and nuance may can be conveyed by speech in a way that is impossible in written communication.”¹²

12. The last section of this paper considers the vulnerabilities of the modern digital battlefield. As former British Air Commodore Timothy Garden writes, an “increasing dependence on highly technical devices makes for a greater vulnerability to effective counter-measures.”¹³ Mattis states that the US Marine Corps’ Achilles’ heel following the Iraq War of 2003 was “overconfidence in uninterrupted communications. In a future war, these communications are certain to be broken. Therefore, we had to know how to continue fighting when (not if) our networks fail.”¹⁴ Indeed, western militaries have recently enjoyed a long period of fortuitously permissive communication environments which has undoubtedly led to complacency and overconfidence. This presents two main vulnerabilities to contemporary operations. First, most modern communication networks and soldier systems have not been sufficiently stressed in disruptive combat conditions. Purveyors of modern military communication and soldier systems may be promising systems which are “unsustainable or useless in war conditions”.¹⁵ Second, adversaries will attack a perceived weakness. Western militaries’ overreliance on communications

¹² *Ibid.*, 592

¹³ Garden, Timothy. *The Technology Trap* (Brassey’s Defense Publishers, 1989), 134

¹⁴ Mattis, *Call Sign Chaos...*, 156

¹⁵ Gordon, *The Rules of the Game...*, 592

technology to effect command and control and achieve information superiority presents a vulnerable target. Technologies available to disrupt or deny modern communication networks (e.g., jamming of satellite communications) continue to proliferate and offers a low-cost and effective countermeasure. Moreover, such ‘below the body-bag count’ actions in the spectrum of conflict may be deemed more politically appealing.

13. There are ample historical examples where new communications technologies, promising to reduce friction in war, failed in the crucible of battle. Noted British maritime historian Andrew Gordon, in his book *The Rules of the Game* provides a thorough study of how wireless telegraphy (W/T), fielded within the Royal Navy in the early 20th century prior to the outset of World War I, failed to live up to its promise during the Battle of Jutland in 1916. Not only did W/T fail to function effectively¹⁶ under the combat conditions, it was also easily jammed by the German High Seas Fleet who exploited the Royal Navy’s vulnerable centralised command and control system to support their escape from the battle. Such an example offers a valuable reminder that commanders will be denied, either by the enemy or otherwise, the communication systems which they come to rely upon during peacetime training.

14. To counter the inevitable communication breakdowns of the digital battlefield, commanders would do well to return to command and control principles which have been tested in the crucible of battle. Nelson understood that signaling systems can and will fail when used in disruptive combat conditions and famously instructed his subordinates, prior to the Battle of Trafalgar in 1805, that “no captain can do very wrong if he places

¹⁶ *Ibid.*, 590

his ship beside that of the enemy.” Mattis emphasized this approach within the US Marine Corps stating that “in future battles, outcomes will depend on the aligned independence of subordinate units...Make your intent clear, and then encourage your subordinates to employ a bias for action. The result will be faster decisions and stronger unity of effort.”¹⁷ It is clear that enduring mission command principles cannot be replaced by the advent of connected warfighters on the digital battlefield; but it is incumbent upon commanders to enforce these principles within their command to avoid the inevitable creep towards overcontrol and centralisation promoted by modern communications.

CONCLUSION

15. The nature of war continues to be characterised by the Clausewitzian trinity of chance, uncertainty, and friction. Modern communication systems should be implemented and employed with these enduring tenets in mind in order to, where possible, reduce the fog of war. The connected warfighter in today’s digital battlefield offers many advantages clearly demonstrated in recent military conflicts where network-centric warfare and information superiority ruled the day against a technologically inept and asymmetric enemy. This paper, however, seeks to remind readers that the proliferation modern communications technology onto the battlefield brings with it a number of pitfalls. Indeed, side-effects such as information overload, insatiable information appetites in headquarters, and acute vulnerabilities to communication systems in combat will, if not properly mitigated, increase friendly friction and thicken the fog of war. Mitigating measures and historical case studies outlined herein offer no

¹⁷ Mattis, *Call Sign Chaos...*, 156

panaceas but remind commanders that new technological systems must be tested in realistic and disruptive combat conditions before being accepted for use in operations.

RECOMMENDATION

16. As with any new military technology, commanders and warfighters must be reminded that modern communication and soldier systems must *serve them* in support of their tasks. This paper has shown rather that warfighters themselves are highly susceptible to becoming servants to the technology in the digital battlefield. Warfighters must learn to leverage modern-day communication technologies and soldier systems to enhance their ability to complete their essential tasks; they must also learn to avoid single points of failure and appreciate that modern systems can and will fail on operations. In other words, warfighters at all levels must be prepared to operate independently from time to time and thrive in unpredictable and chaotic situations directed by clear commander's intent. Such discomfort can be somewhat alleviated by realistic training and doctrine. Militaries must also learn to stress command and control, and communication systems, under realistic disruptive combat conditions to expose dependencies and friction. Moreover, militaries should never associate 'normal' with 'peacetime' conditions by which communication systems are routinely vetted.

17. In today's ever connected world of high speed military networks, it is refreshing to consider military functions which do not rely on 'always-on' communications in the performance of their functions. Such is the example of submariners who covet the ability to work independently and, once on station, can go hours and even days without sending or receiving updates. It is a reminder that the effectiveness of command and control is not

linked to the communication systems employed; nor that signals activity is any indicator of military achievement.

BIBLIOGRAPHY

Dunnigan, James F. *Digital Soldiers*. Macmillan, 2001.

Ferris, John, and Michael I. Handel. "Clausewitz, Intelligence, Uncertainty and the Art of Command in military operations." *Intelligence and National Security* 10, no. 1 (1995): 1-58.

Garden, Timothy. *The Technology Trap*. Brassey's Defense Publishers, 1989.

Gordon, Andrew. *The Rules of the Game: Jutland and British Naval Command*. Naval Institute Press, 2013.

Martin, John, Laurel Allender, Pamela Savage-Knepshield, and John Lockett, eds. *Designing Soldier Systems: Current Issues in Human Factors*. CRC Press, 2018.

Mattis, Jim, and West, Bing. *Call Sign Chaos: Learning to Lead*. New York: Random House, 2019.

Shanker, Thom, and Richtel, Matt. "In New Military, Data Overload Can Be Deadly." *The New York Times*, January 16, 2011. Accessed 24 October, 2019.
<https://www.nytimes.com/2011/01/17/technology/17brain.html>

Woodward, Sandy, and Patrick Robinson. *One Hundred Days*. London: Harper Press, 2012.