CANADIAN FORCES COLLEGE / COLLÈGE DES FORCES CANADIENNES

AMSC 5 / CSEM 5

INFORMATION AGE COMMAND AND CONTROL – THE WEAKEST LINK?

By Colonel Manfred H. H. Arndt

ABSTRACT

This paper examines the evolution of information technology and its impact on the conduct of warfare. Information technology has permeated every facet of military operations and the military has become utterly reliant on information technology for virtually all aspects of administration, management, support and warfare. Of particular significance is the impact of information technology on command and control. Modern command, control and information (C^2I) systems provide commanders with an unprecedented amount of real time or near-real time information. If this information is managed and used correctly, it will provide the commander with a remarkable advantage. If managed or used incorrectly, it could have devastating consequences. In the current age of high speed precision guided weapons, almost instantaneous reactions are required in order to defeat an adversary's weapons. This can only be effectively executed via ever-increasing degrees of remote control and even automation. The paper argues that limitations of information technology, the military's total reliance on it, numerous inherent vulnerabilities, and a virtual absence of redundancy or back-ups systems/processes all serve to create a serious weakness in the military which could be readily exploitable by an adversary.

INFORMATION AGE COMMAND AND CONTROL – THE WEAKEST LINK?

By Colonel Manfred H.H. Arndt

INTRODUCTION

> *…while up-to-date technical means of communication and data processing are absolutely vital to the conduct of modern war in all its forms, they will not in themselves suffice for the creation of a functioning command system, and that they may, if understanding and proper usage are not achieved, constitute part of the disease they are suppose to cure*.
>
> - Martin van Creveld, 1985

Throughout history there has always been an interesting link between "war-fighting" and technology. Which one has driven the other has varied often depending on the time in history or the technological area involved. In the current era of exponentially increasing technological development, there is no area that has had a greater impact than that of information technology. Advancements in information technology have had a profound effect on the military. The increasing complexity of military weapons systems, military organizations and war-fighting itself, have created an ever-increasing demand for and reliance on information technology systems. Highly efficient logistical support for modern weapons systems is paramount to their effectiveness. The complexity of systems demands specialized support personnel. The size/complexity of the battlefield, almost limitless variety of threats, as well as increasing emphasis on ethical, political and legal factors have served to phenomenally increase the quantity of information with which a commander and his staff must contend. As a result, ever-increasing demands on

automation are being made in order to maintain some reasonable ratio of "war-fighters" to support/command personnel.

Advanced Command, Control and Information (C^2I) systems are touted to be the enablers and "force multipliers" that will give modern armed forces the decisive edge over potential adversaries. It will be argued, however, that the inherent weaknesses and complete dependency on information technology in modern military C^2I systems have created a critical vulnerability that must be addressed.

INCREASING COMPLEXITY OF WARFARE

Throughout history until the Middle Ages, a commander directly led his relatively small number of troops in combat. "He could see the entire battlefield and give orders directly to his troops."[1] As the number of combatants grew, and weapons increased in range, accuracy and firepower, the battlefield became too large and complex for a commander to directly observe and coordinate the activities of his troops. He could no longer single-handedly plan, coordinate, and lead his forces, let alone administer day-to-day logistic and personnel requirements. Special staffs were required to manage the ever-increasing magnitude of information flow.[2] The growth of the German Bundeswehr Staff by well over an order of magnitude over the last century or so[3], as well as an equivalent increase in support staff to maintain complex weapons systems,[4] serves to put the increase in staff requirements into context. Clearly, the exponentially decreasing ratio

[1] Arthur F Huber et al., The Virtual Combat Air Staff – The Promise of Information Technologies (Santa Monica: Rand, 1996), 11
[2] Ibid., 11
[3] Martin van Creveld, Technology and War – From 2000 BC to the Present (New York: The Free Press, 1989), 236-237

of combat personnel to support personnel had to be addressed or there would soon be no combat troops left to fight.

APPLICATION OF INFORMATION TECHNOLOGY

Although varied in their responsibilities, the main function of staffs was to collect, process, and transmit information. Martin van Creveld in his analysis of the Vietnam war stated that "Extreme specialization of personnel and of units, coupled with adherence to the traditional triangular chain of command, meant that headquarters was piled on headquarters and that coordination between them could only be achieved, if at all, by means of inordinate information flows."[5] Technical evolution, the same factor responsible for generating a significant portion of the staff requirement through its resultant increased complexity, promised a potential solution. The evolution of computer (information) technology gave rise to the opportunity to automate many staff functions. "As the military of many countries strove to automate their operations during the 1950's, the first fields to be affected were personnel administration, record keeping, and many aspects of logistics such as requisitioning, and keeping track of spare parts – in brief, "the Business of war"…"[6] Once employed by the military, information technology permeated virtually every function. "Due to the sheer size of armed forces as compared to virtually all other social organizations, automation represented the only way for it to be administered anywhere near the efficiency of other organizations."[7] After the integration

---

[4] Martin van Creveld, Command in War (Cambridge: Harvard University Press, 1985), 234-35
[5] Ibid., 258
[6] Martin van Creveld, Technology and War, 240
[7] Ibid., 239

of information technology for administrative and logistic purposes became prevalent, it began to infuse the field of communications through the automation of switchboards. Computerized switchboards in turn lead to the linking of computer systems employed by various parts of the organization.[8] These networks formed the basis for the evolution of modern logistic/administrative management and C^2I systems. These networked systems did not always initially fulfill user expectations. Sometimes appearing as if there was an unguided drive to apply IT to ever-increasing C^2I applications in the military, many systems withered into extinction or were severely limited in scope because they did not meet the needs of the chain of command.[9] As shortcomings were addressed and commanders became more and more aware of the capabilities of C^2I systems, they generated an ever-increasing demand for greater amounts and more up-to-date information. Van Creveld declares that the history of warfare is an endless quest of decreasing the "realm of uncertainty, resulting in a race between more information and the ability of technology to keep up with it."[10]

THE LURE OF CENTRALIZED CONTROL - THE REMOTE CONTROL BATTLEFIELD

Technological developments that enabled near-real-time communications farther than the in-air transmission of voice or visual line-of-sight signals, fundamentally altered

[8] Ibid., 240
[9] The Canadian Air Force initiated the deployment of a number of C^2I systems over the last two decades; none have become the all encompassing systems that they were to have become; many were abandoned while those that survived tended to fill niche/stovepipe requirements.
[10] Qtd. in Frank M Snyder, Command and Control: The Literature and Commentaries (Washington: National Defense University Press, 1993), 148

the exercise of command and control in warfare. "The telegraph and subsequent developments enabled commanders thousands of miles away to maintain an electronic battlefield presence and eventually coordinate theatre-wide operations."[11] However, this capability in turn again generated a requirement for increased information. Van Creveld stated that: "A tendency towards centralization, the pooling of resources, and the running of the war by remote control – especially evident in the field of logistics and in the air war against North Vietnam – further augmented the demand for information."[12]

A strong, centralized hierarchy has always been the foundation of military organizations. The phenomenal increases in the complexity of modern-day warfare, however, make strict adherence to this principle utterly unworkable. Gregory Roman stated: "Unfortunately, the greater the level of control, the less opportunities for initiative and flexibility where it is needed most to cope with the dynamics of warfare: at the lower levels of command."[13] Van Creveld summarized it well when he stated: "The paradox is that, though nothing is more important in war than unity of command, it is impossible for one man to know everything. The larger and more complex the forces he commands, the more true this becomes."[14] Information technology offers the opportunity for shared real-time information across all levels of command. While centralized strategic command can (and indeed should) be retained, control of operations must be decentralized to the maximum extent possible at all levels. Given appropriate empowerment, lower-level

[11] Donald E Ryan Jr., "Implications of Information-Based Warfare," Joint Force Quarterly Autumn/Winter 94/95, 114
[12] Martin van Creveld, Command in War, 258
[13] Gregory A Roman, "The Command or Control Dilemma – When Technology and Organizational Orientation Collide," Air War College Maxwell Paper No 8, 10
[14] Martin van Creveld, The Transformation of War (New York: The Free Press, 1991), 109

commanders could then exploit this information to maintain an ops tempo hopefully sufficient to defeat the enemy. However, this decentralization of control, which is deemed essential to the successful conduct of Information Age warfare, does not appear to be happening. As Roman states: "The seductiveness of information technology stimulates military organizational orientation towards greater centralized control and more rigid hierarchical organizations instead of the desired orientation of decentralized control and more flexible organizations."[15] He goes on to warn: "Unless the US military recognizes the danger of succumbing to technological temptation, control functions may take priority over command functions, resulting in both a less efficient and less effective military."[16]

NETWORK CENTRIC WARFARE – THE AUTOMATED BATTLEFIELD

We have not yet fully grasped or dealt with the limitations of remote control warfare, yet the application of technology is resulting in ever-increasing degrees of automated warfare. "In the US Strategic Defense Initiative, one of its most complex features, battle management, would be the responsibility of an elaborate network of computers."[17] Although some may argue that the end of the Cold War will delay or eventually kill this project, there are already many examples of fully automated systems in existence today "…such as the Navy's Phalanx close-in air defense weapon, which is capable of autonomously performing its own search, detect, evaluation, track, engage,

[15] Gregory A Roman, 3
[16] Ibid., 3

and kill assessment functions."[18] "In short, the military systems (including weapons) now on the horizon will be too fast, too small, too numerous, and will create an environment too complex for humans to direct. Furthermore, the proliferation of information-based systems will produce a data overload that will make it difficult or impossible for humans to directly intervene in decision making."[19]

The current trend towards network-centric warfare involves the linking of numerous sensors and weapons platforms via a sophisticated and highly automated C^2I system. "Network-centric warfare is more than just technology. It's the massing of the effects of long-range fire rather than the massing of forces. … The capability to strike effectively without massing forces creates significant advantages for ships, aircraft and ground troops hindered by requirements for forward bases, logistical tails, and coalition hosts."[20] With this advantage, however, come several side effects. Once again there is an increased demand for C^2I system sophistication; by necessity many response actions must be automated and there is virtually no effective backup.

The C^2I systems involved in this type of warfare would have to detect targets, classify priorities, select weapon types, select weapons platforms, and determine engagement criteria. In order to optimize effectiveness, most of these functions would have to be completely automated. It is inconceivable how a commander, responsible for

---

[17] Mervyn Berridge-Sills, "Computers and Stategy: It's the Thought that Counts" The Changing Face of War, ed.Allan D English (Montreal & Kingston: McGill University Press, 1998), 185 and Lee Hassig Ed. Understanding Computers – The Military Frontier (Alexandria: Time-Life Books, 1991), 112
[18] Thomas K Adams, "Future Warfare and the Decline of Human Decisionmaking," Parameters, US Army War College Quarterly, Winter 01-02, 57
[19] Ibid., 58
[20] William K Lescher, "Network Centric: Is it Worth the Risk?," Proceedings, Jul 99, 58-59

a particular weapons platform, would have any meaningful input into the decision making process. Even if all of the information used to make the engagement determinations were available to him in real time, response time constraints would not permit any degree of analysis, challenge or confirmation. It is also inconceivable how any higher level of command could exercise any meaningful control other than setting limits or "turning the system on or off". The complexity of the battlefield and the time constraints involved would permit virtually no effective backup to the detection, classification, and engagement of targets. It would take an enormous well-integrated and well-trained battle staff to even come close. Under network-centric warfare, however, any remaining "battle-staff" would only exist in the virtual "network-centric" realm. Without the information technology to tie them together, they would effectively not exist at all. Also, because the basic approach of network-centric warfare involves an "electronic" or "virtual" concentration of force, no effective backup for this exists either. If the C^2I system is degraded or unserviceable, physical concentration of force will be unachievable due to time-distance factors involved.

ABSOLUTE DEPENDENCE ON INFORMATION TECHNOLOGY

Reliance on information technology has spread throughout all facets of the conduct of warfare. From personnel administration, through logistics, finance, intelligence and down to the tactical direction on the battlefield itself, each of these functions hinges, to ever-increasing degrees, on information technology. A mere 15 years ago, the vast majority of formal military communications at the operational level

and above were still conducted via letter or, for matters of greater urgency, via the military message system. Today the vast majority of communications are conducted in a much less formal fashion via e-mail, fax, telephone and sometimes just keyboard entries on the defence wide area network (DWAN).[21] Although seemingly cumbersome, the previous system did provide some advantages. Signed paper copies of all correspondence were logged and filed thereby providing a permanent record of authority and accountability. Depending on the urgency and/or sensitivity of a message, several other methods of transmission could be utilized if the message handling system was temporarily down. The message could be faxed, hand-carried, or read verbatim over the telephone (to be followed up by paper copy). Today, with the unofficial nature of most e-mail correspondence, it is often impossible to determine whether the content is a request, suggestion or formal direction (order). The record of accountability is tenuous at best and there is no backup if the DWAN system is down. Most offices no longer even have the capability to generate "paper" correspondence without the support of automated data processing equipment. It is true that our computer networks have enjoyed great reliability overall, but they have been off-line due to viruses and other technical issues. One must also remember that they are not currently under attack. It is not suggested that we return to the past. We do, however, need to clearly analyze needs, develop robust solutions, understand weaknesses, and identify work-arounds to critical vulnerabilities if we wish to avoid the paralysis that we have experienced with the occasional loss of connectivity to-date.

[21] The DWAN is the Canadian Forces' nation-wide unclassified computer network which is increasingly being used to handle personnel administration, financial management, logistics management, and

The impact of total reliance on information technology for administrative purposes is significant enough, but what about the impact on battle management. Are we prepared to take a "time out" on the battlefield because our systems are temporarily down? Although seemingly far-fetched, the reality is that we would have to do just that. Peacetime exercises have demonstrated time and time again, that the loss of even basic communications, results in "op tempo" grinding to a halt. Communications jamming during exercises is generally severely restricted or prohibited completely because commanders and exercise directors feel that little useful training could be achieved if communications were disrupted.

In today's modern militaries, information technology is no longer a "force multiplier" it is a basic "force enabler". Without information technology, all operations would quickly be severely degraded or come to a complete halt. Donald Ryan summarized it well when he wrote: "information technology has increased in complexity and become indispensable to combat operations – so pervasively that modern militaries are utterly dependent upon it to maintain, deploy, and employ virtually every weapon system in their arsenals."[22]

VULNERABILITY OF C^2I SYSTEMS

From the earliest days of electronic communications, military reliance on information technology was fraught with risk. Barbara Tuchman stated, that during the

---

communications.
[22] Donald E Ryan Jr., 114

execution of the Schlieffen Plan in August 1914: "Nothing caused the Germans more trouble, when they were operating in hostile territory, than communications."[23] Commenting on the evolution of information technology and its impact on command and control half a century later, van Creveld stated "To study command as it operated in Vietnam is, indeed, almost enough to make one despair of human reason; we have seen the future and it does not work."[24] Despite these lessons (not) learned through history, we have done precious little to address C^2I system weaknesses.

The simplest threat against C^2I systems is direct physical attack. A relatively recent example was highlighted by Donald Ryan: "During DESERT STORM, the piecemeal destruction of Iraqi forces was made possible by paralyzing its central nervous system – that is C^4I Links."[25] Precision guided weapons used against key communication nodes and command centers virtually eliminated the possibility of any type of coordinated defence or counter-attack. There is nothing that makes western allied forces immune from this. In fact, the greater sophistication of and reliance on these systems make them more vulnerable. Despite their critical nature, military C^2I systems rely heavily on commercial infrastructure. Some systems use the public internet as their conduit, while other systems (both encrypted and unencrypted) rely on normal telephone switching stations and landlines. We have undoubtedly fallen into a false sense of security in that operations in Iraq, the former Republic of Yugoslavia, and now Afghanistan have been conducted against enemies virtually devoid of the resources necessary to be a real threat to our information systems.

[23] Barbara W Tuchman, The Guns of August (New York: Macmillan, 1962), 214
[24] Martin van Creveld, Command in War, 259

C^2I systems could also fall victim to a myriad of indirect attacks. The current and future dependency of C^2I systems on commercial off-the-shelf (COTS) technology will make potential exploitation by an adversary significantly simpler. "The equipment could be purchased on the open market and an adversary could then 'learn how to break it'."[26] This could be accomplished by exploiting either its hardware or software weaknesses.

Considerable potential exists in the realm of Cyber Warfare involving the transmission of "Cyber bombs" over the system's normal transmission media. A particular concern is that this type of warfare is not limited to highly funded and highly trained experts. A serious hacker with access to relatively simple equipment could wreak serious havoc on information system networks. Viruses with a variety of effects are "… capable of sabotage and electronic 'guerrilla' action behind enemy lines.[27] Special "sleeper" viruses could be inserted into a potential adversary's C^2I system, left dormant, and called into action when needed[28]

Closely associated with targeted "denial of service" is the issue of information security. Emmett Paige Jr., then Assistant Secretary of Defense for Command, Control, Communications and Intelligence stated: "One of our greatest challenges to creating a new information system to support the war fighter is how to maintain security of the information. … The vulnerability to C^4I systems and networks is increasing as data flow

---

[25] Donald E Ryan Jr., 114
[26] Ibid., 114-115
[27] Ibid., 115
[28] Ibid., 115

is simplified. … As our war fighters become more and more dependent on our information systems the potential for disaster is obvious."[29] Put simply, even the most sophisticated C^2I systems can be rendered useless if the data they contain, act on, or present to users, cannot be trusted. Equally critical, is the potential for an adversary to exploit information gleaned on own force strengths, dispositions, etc. Although key command systems may be protected by firewalls and encryption, a remarkable amount of crucial logistics support information and personnel administration continues to be conducted via unclassified systems. "During the Gulf War a Dutch hacker managed to pull a great deal of critical information on US forces, strengths, and dispositions from unclassified DOD computer systems."[30]

Another potential area of attack is the human interface with C^2I systems. mp

computer operators into a trance. The subconscious perception of the new pattern eventually results in arrhythmia of the heart. Other Russian computer specialists confirm this 25th frame effect and its ability to inject a thought into the viewers subconscious."[32]

The vulnerabilities discussed thus far all involve some direct action by an adversary. C^2I systems, however, also have other inherent limitations that require no specific action by an adversary to exploit. A crucial limitation is the rate at which the human mind can process information presented on a display. Although information technology power has increased by an order of magnitude every several years, the human mind's ability to process inputs has remained virtually unchanged for thousands of years.[33] The basic ability of the human mind to process text has been assessed by some researchers to be in the order of 1000 bits per minute. It has been suggested that this rate can be increased by a factor of approximately five with appropriate training and subject familiarity.[34] Dr James Wise, staff scientist in the information science department of the Pacific Northwest Laboratory believes that significant increases in human processing ability may be realized by changing the fashion that data is presented. He contends that the brain processes visual image information differently from text based information. Visual interpretation is done pre-consciously and sent throughout the visual cortex. This results in visual information being processed at least 100 times faster than textual information.[35] Even with this theoretical increase of two orders of magnitude, it is still a far cry from information technology systems with a bandwidth that is many thousands of

[32] Ibid., 86
[33] William P Gruner, "No Time for Decision Making," US Naval Institute Proceedings, (1990), 40
[34] Ibid., 40
[35] Andrew C Braunberg, "Brain's Affinity for Imagery Eases Information Overload," Signal, Dec 96, 49

times greater. Robert Bateman III raises an interesting question with respect to information overload: “Because information requires decisions, and decisions require time, what happens to our speed through the ODOA cycle when the information potential is increased beyond available time?”[36]

Other factors can also affect the effectiveness of the human-system interface. The complexity and user-friendliness of C^2I systems can severely affect their utility even when the rates of data flow are not excessive. Van Creveld comments on the systems in use during the Vietnam War: “Confronted with a military information network that was impossibly complex and in the end often unable to cope, decision makers not unnaturally responded by attempting to cut through by any and every means that presented themselves.”[37] An even more vivid exampaET4beite opaEin-depth s

s a

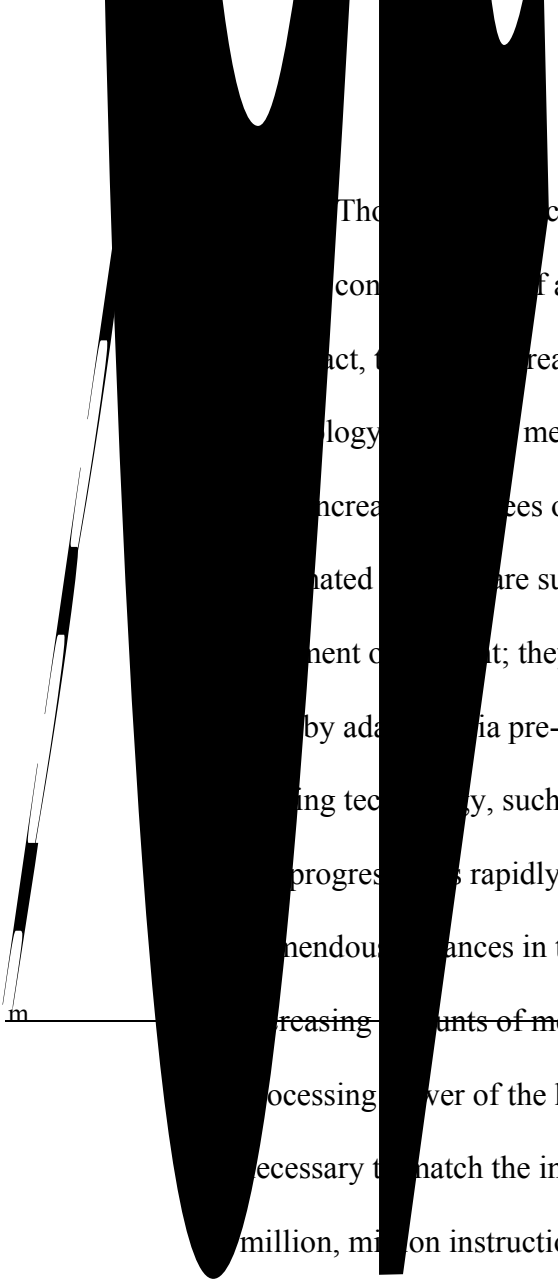
In an attempt to address issues of high data rates, reducing response times, and unworkable human-system interfaces, designers have incorporated ever-increasing degrees of automation into their C^2I systems. During the Cold War a key element of Mutual Assured Destruction was the confirmation of enemy missile attack early enough to permit a counter-attack against the enemy. The NORAD C^2I system incorporated the most powerful computing capability of the day. "On 5 November 1960, the US ballistic missile early-warning system (BMEWS) detected a 99.9 percent certainty of a massive Soviet missile attack, which turned out to be the rising moon."[40] Luckily, the final decision to launch required human interaction as 99.9 percent would undoubtedly have been set as sufficient criteria for automated response. Interestingly, this last step human interaction was also felt to have rendered the system ineffective had a real attack actually been in progress. Van Creveld stated: "Throughout the sixties and seventies, the automatic battlefield has been the subject of much speculation. Things have not yet proceeded that far, in large part because many potential war environments turned out to be much too complicated to be 'understood' even by the best available computer programs."[41] He further summarized the limitations of computerized systems: "Electronic sensors and the computers to which they are hooked cannot match the human brain in flexibility and inventiveness. They find it very hard to tell friend from foe, real targets from decoys, worthwhile objectives from every kind of clutter. They can also be

[40] Alan Borning, "Computer System Reliability and Nuclear War," Communications of the ACM, Vol 30 No 2, (1987): 126
[41] Martin van Creveld Technology and War, 241

jammed, overloaded, or spoofed, often by cheap devices freely available on the open market."[42]

Despite inherent limitations of automation, this trend is increasing due to necessity. The small size, increased speed and amazing accuracy of modern weapons require very quick responses if defence is to be effective. Automatic systems have been in use for years at the tactical level. A common application has been in the self-defence role onboard aircraft, ships and vehicles. Responding to an immediate threat, these systems provide immediate warning, control jamming countermeasures, and deploy expendable countermeasures (chaff/flares). In the worst case, if these systems failed or resulted in an inappropriate response, the consequences were acceptable. If Tc -cum(h)Tj12 0 0 52 2 4 196785

ontrpotentially



Tho contends: "The fundamental development underlying the loss of con f automated information systems."[43] One could also argue that it act, t reasing amount of information available through information logy meaningful human decision making impossible, thereby leading to ncrea ees of automation. In either case, the important issue is that nated are subject to limitations of their programming. They are incapable of ment c t; they have no experience and, to date, they do not really learn other by ada ia pre-programmed logic. "Unfortunately, advances in decision-ing tec gy, such as computer assisted logic tools and artificial intelligence, have progres s rapidly as information gathering technology."[44] Despite the mendou ances in technology resulting in ever-faster processing power and reasing unts of memory, the computers of today still fall well short of the ocessing wer of the human brain. The processing power and memory capacity ecessary t match the intellectual power of the human brain has been estimated at 100 million, mi on instructions per second (100 million MIPS). Research and development efforts have identified the technologies that will permit advances in computing power to these levels. The current trend of computer evolution is expected to result in affordable machines with this capacity being available in the 2020's.[45] When these machines become available, it will be interesting to see if they will be the super-brains expected, or whether they will be as bogged down and limited by human qualities such as

[43] Thomas K Adams, "Future Warfare and the Decline of Human Decisionmaking," Parameters, US Army War College Quarterly Winter 01-02, 58

[44] Gregory A Roman, "The Command or Control Dilemma – When Technology and Organizational Orientation Collide," Air War College Maxwell Paper No 8, 12

[45] Hans Moravec, "When Will Computer Hardware Match the Human Brain," Journal of Evolution and

contemplation, reflection, second-guessing, uncertainty, etc. as is the human brain. Going a step further yet – will computers have personalities? Will there be "bad" machines with a "mean streak" and "compassionate" machines incapable of harming anyone or anything? Although still currently in the realm of science fiction, the next 20 to 30 years may provide more insight. In the meantime, it seems that the only way to maintain meaningful human decision making and control is by accepting a slower information processing rate. Without doubt, however, an adversary will inevitably decide that the way to defeat the human-centric system is by attacking it with a system that is not so limited.[46]

Yet another insidious vulnerability resulting from the proliferation of information technology is the disappearance of redundancy and/or backups. This aspect was most clearly illustrated during preparations for Y2K, when the realization took place that virtually all of our day-to-day requirements: (transportation (cars, rail, air, bus, subway); communications (telephone, radio, television); utilities (electricity, gas, water); shopping, appliances; etc.; etc. were all controlled, to some degree or another, by computers. Even more eye opening was the fact that in most cases mechanisms no longer existed to deliver these requirements without their integrated computer support. In the military realm, the impact of loss of connectivity and/or communications has already been discussed. Are we so naïve as to believe that we could never face an adversary with the technical capabilities to disrupt our information technology systems? I would suggest, once again, that we err in assuming that operations in Iraq, the former Republic of Yugoslavia, and

[46] Thomas K Adams, "Future Warfare and the Decline of Human Decisionmaking,"

now Afghanistan, conducted against enemies with limited high-tech resources, are reflective of all potential future conflicts.

Redundancy and backups can take many forms. We naturally tend to think of alternate technical means to provide "electronic" connectivity. The following examples may serve to expand the context of redundancy and backups. Increasingly the shipment of material is being automated. Specific items are collected, packaged, shipped, tracked and received using automated processes. Without the information available from information technology systems, a critical component for a weapons system may already be available in some container in the theatre of operations but cannot be located because paper inventory sheet backups no longer exist. Another example involves the military staff at the various levels of headquarters. As previously illustrated, the size of military staffs grew, as warfare became more complex and involved ever-increasing amounts of information flow. When this was no longer workable, automation was employed to execute functions previously carried out by staff. Taken to the extreme, however, in commercial corporations, automation can eliminate entire levels of management. "In a corporation organized as a network, middle management positions disappear as two of their main functions – information transfer and worker supervision, dissipate."[47] Although the military's hierarchical traditions tend to slow down this trend, fiscal realities are allowing no other choice. The problem with the associated loss of staff is that when the automated systems fail or degrade the personnel for even limited manual human backup no longer exist.

A common approach to assessing superiority or vulnerability is comparison of one's capabilities with those of potential adversaries. The problem with this approach is that it is relevant only when the adversary engages you in a similar (symmetric) fashion. Donald Ryan Jr. wrote: "not every adversary in potential conflicts (for instance, low intensity conflict in the Third World) will be as information-dependent as technologically advanced nations. This is a legitimate observation; but it overlooks the fact that technologically advanced, information intensive military organizations are more vulnerable to information warfare simply because they are information-dependent. … An adversary need not be information-dependent to upset our information lifeline."[48]

Asymmetric/non-traditional warfare will undoubtedly add even greater challenges. Threats or attacks by non-state organization may require a great deal of coordination with other government agencies such as the Solicitor General, Foreign Affairs, Customs, Immigration, Communications, Transportation or even Fisheries. The United States has had some experience in this area in its extended war on terrorism.[49] Less well known are our own Canadian experiences involving counter-narcotic, illegal immigrant and illegal fishing operations.[50] In all cases, it quickly became evident that incompatibilities in policies, structure and equipment placed significant challenges on

---

[47] Gordon R Sullivan & James M Dubik, "War in the Information Age," Military Review, Apr 94, 51
[48] Donald E Ryan Jr., 114-115
[49] Although the "War Against Terrorism" was officially declared by President Bush during the aftermath of 11 Sep 01, this war actually started decades earlier in response to numerous and varied terrorist attacks against US interests.
[50] The author was attached to Comd MARLANT's staff as a planning officer during the Canada-Spain "Turbot War" in the Spring of 95 and was involved in the coordination of numerous counter-narcotic and illegal immigrant operations as the 19 Wing Operations Officer (1999-2002)

operations. "Quick, flexible interagency coordination will also be necessary at the operational level."[51]

CONCLUSIONS

Whether the military was part of the reason for its development or it simply applied available capabilities to address its requirements, information technology has become an integral and essential part of the military institution. The military could no more function without information technology than a human could survive without air. The support of modern high-tech weapons systems, effective administration of diverse and highly specialized personnel, and control of an ever-increasingly complex battlefield can only be accomplished with the aid of significant information technology. This reliance on information technology has fundamentally changed the face of modern warfare. On the battlefield a bigger and better bang has taken a backseat to miniaturization, precision and instant reaction times. A clear real-time picture of the enemy and his actions has become paramount to the effective use of these modern weapons.

The reliance on these systems demands that they be as robust and dependable as absolutely possible given realistic financial restraints. Systems should be designed to employ a shared network structure versus a hierarchical structure that would render them subject to single node failure. They must incorporate degraded mode operation and have

[51] David Tucker, "The RMA and the Interagency: Knowledge and Speed vs. Ignorance and Sloth," Parameters, US War College Quarterly, Autumn 00, 67

the flexibility to automatically or easily be re-configured to employ alternate modes of connectivity.

In some areas of warfare, the amount of information required in order to respond appropriately and/or the extremely short reaction times required, will demand fully automated systems. These systems must be designed, and tested, with the greatest rigor possible to ensure they function in the manner expected. Since machines cannot yet understand "the will of the commander", it is crucial that all essential elements of human decision making are incorporated into their construction, their programming and their activation.

In other areas of warfare where human intervention is still required, the emphasis on obtaining information to achieve complete "knowledge" will be so great that information overload will be a constant threat to commanders. In the quest for perfect information they may unwittingly place themselves in the position of having lost the big picture. Once in this state, the commander no longer serves a useful purpose with respect to the effective direction of operational activities. Information technology must be effectively managed and filtered in order to optimize its utility at any level.

Information technology will allow every bit of information to be available in real time at virtually every level. In addition to the threat of information overload, there remains the ever-present opportunity for higher-level commanders to micro-manage the activities at lower levels. Commanders must avoid limiting or bypassing the decision

making opportunities of those closest to and most capable of handling activities at their level.

Lastly, all systems remain subject to failure. We must retain or re-adopt lower-tech backups or workarounds and we must periodically exercise them. If an adversary assesses our C^2I systems to be our weakness, he will undoubtedly expend significant energy on disrupting them. As highlighted herein, there is no shortage of vulnerabilities that an adversary could exploit.

Bibliography

Ackerman, Robert K. "Visualizing Information Emerges as Major Element of Operations." Signal, Feb 99, 17-19

Adams, Thomas K. "The Real Military Revolution." Parameters, US Army War College Quarterly, Autumn 00, 54-65

Adams, Thomas K. "Future Warfare and the Decline of Human Decisionmaking." Parameters, US Army War College Quarterly, Winter 01-02, 57-71

Adams, Thomas K. "Radical Destabilizing effects of New Technologies." Parameters, US Army War College Quarterly, Autumn 98, 99-111

Bateman, Capt Robert III. "Avoiding Information Overload." Military Review, Jul-Aug 99, 53-58

Berridge-Sills, Mervyn. "Computers and Strategy: It's the Thought that Counts." The Changing Face of War. Ed. Allan D English. Montreal& Kingston: McGill University Press, 1998. 181-196

Borning, Alan. "Computer System Reliability and Nuclear War." Communications of the ACM Vol 30 No 2 (1987): 112-131

Braunberg, Andrew C. "Brain's Affinity for Imagery Eases Information Overload." Signal Dec 96, 49-51

English, Allan D. "Contemporary Issues in Command and Control." an essay based on a paper prepared for the Deputy Chief of Defence Staff retreat held in Kingston, ON in Feb 2001.

FitzSimmonds, James R. "The Cultural Challenge of Information Technology." NWC Review Summer 98. [journal online]. Accessed 3 Oct 02. Available from http://www.nwc.navy.mil/press/Review/1998/summer/art1su98.htm

Gruner, William P. "No Time for Decision Making." US Naval Institute Proceedings (1990): 39-41

Harley, Jeffrey A. "Information, Technology, and the Center of Gravity." [journal online]. Accessed 3 Oct 02. Available from http://www.nwc.navy.mil/press/Review/1997/winter/art4wi97.htm

Hassig, Lee, Ed. Understanding Computers – The Military Frontier. Alexandria: Time-Life Books, 1991.

Huber, Arthur F., et al. The Virtual Combat Air Staff – The Promise of Information Technologies. Santa Monica: Rand, 1996

Keegan, John. A History of Warfare. Toronto: Key Porter Books, 1993.

Killion, Thomas H. "Decision Making and the Levels of War." Military Review Nov-Dec 00, 66-70

Lescher, William K. "Network Centric: Is it Worth the Risk?." Proceedings Jul 99, 58-63

Metz, Steven. "The Next Twist of the RMA." Parameters, US War College Quarterly Autumn 00, 40-53

Moravec, Hans. "When Will Computer Hardware Match the Human Brain." Journal of Evolution and Technology 1998 Vol 1 [journal online]. Accessed 29 Sep 02. Available from http://www.transhumanist.com/volume1/moravec.htm

Naisbitt, John and Aburdene, Patricia. Megatrends 2000 – Ten New Directions for the 1990's. New York: William Morrow and Company, Inc., 1990.

Paige, Emmett Jr. "From the Cold War to the Global Information Age." Defense Issues Vol 10, No 34, Feb 1995 [journal online]. Accessed 3 Oct 02. Available from http://www.dtic.mil/defenselink/pubs/di95/di1034.html

Pigeau, Ross & McCann, Carol. "Re-conceptualizing Command and Control." Canadian Military Journal Vol 3, No 1 (Spring 2002): 53-63

Roman,Gregory A. "The Command or Control Dilemma – When Technology and Organizational Orientation Collide." Air War College Maxwell Paper No 8 Feb 98

Ryan, Donald E Jr. "Implications of Information-Based Warfare." Joint Force Quarterly Autumn/Winter 94/95, 114-116

Schmitt, John F. "Command and (Out of) Control: The Military Implications of Complexity Theory." Complexity, Global Politics, and National Security [journal online]. Accessed 3 Oct 02. Available from http://www.ndu.edu/inss/books/complexity/ch09.html

Schmitt, John F. "How We Decide." Marine Corps Gazette Oct 95, 16-20

Snyder, Frank M. Command and Control: The Literature and Commentaries. Washington: National Defense University Press, 1993.

Sullivan, Gordon R and Dubik, James M. "War in the Information Age." Military Review Apr 94, 46-62

Thomas Timothy L. "Kosovo and the Current Myth of Information Superiority." Parameters, US War College Quarterly Vol 30 No 1 Spring 00: 13-29.

Thomas, Timothy L. "The Mind Has No Firewall." Parameters, US War College Quarterly Spring 98, 84-92

Tuchman, Barbara. The Guns of August. New York: Macmillan Press, 1962.

Tucker, David. "The RMA and the Interagency: Knowledge and Speed vs. Ignorance and Sloth." Parameters, US War College Quarterly Autumn 00, 66-76

Van Creveld, Martin. Command in War. Cambridge: Harvard University Press, 1985.

Van Creveld, Martin. "High Technology and the Transformation of War – Part 1." RUSI Journal Oct 92, 76-81

Van Creveld, Martin. "High Technology and the Transformation of War – Part 2." RUSI Journal Dec 92, 61-64

Van Creveld, Martin. Technology and War – From 2000 BC to the Present. New York: The Free Press, 1989.