CANADIAN FORCES COLLEGE / COLLÈGE DES FORCES CANADIENNES
CSC 29 / CCEM 29

EXERCISE / EXERCICE NEW HORIZONS

TITLE/TITRE: – Global Command and Control System Development and Human Factors

By / par Maj Rick Dollesin

This paper was written by a student attending the Canadian Forces College in fulfilment 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.

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.

ABSTRACT

Throughout the 1990's the United States Department of Defense has faced both declining budgets and a drawdown in its military forces. To continue to provide 'light, lean, and lethal' combat capabilities, the United States has turned to advances in technology as a leveraging source to support military operations. The evolution of a 'system of systems,' the Global Command and Control System, is the information system that the United States has come to depend on to consolidate a multitude of legacy systems onto a single information system platform. Although security of the Global Command and Control System's data and information is a top priority concern for system developers, human ingenuity and other factors cannot be overlooked.

This essay will use the Global Command and Control System as a case study to examine how human factors or behaviors can affect limitations and vulnerabilities on command and control communications systems and what system developers and users can do to combat those effects. Without a thorough knowledge of human factors and behaviors, a command and control system of systems could be destroyed, or even worse, exploited to level out future battlefields.

> ***If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer defeat. If you know neither the enemy nor yourself, you will succumb to every battle.***
>
> **– Sun Tzu, *The Art of War* (circa 490 BC/1910, pp. 24-25)**[1]

As the United States military progresses through its evolutionary process of technology dependent transformation, the protection of its state-of-the-art secure communications capabilities is increasingly important. "Minor powers, rogue states, and non-state actors" are focusing more on exploiting the vulnerabilities of communications systems; a critical center of gravity for a high-tech military force.[2] Moreover, Richard Clarke, national coordinator for security, counterterrorism, and infrastructure protection in the Clinton administration, emphasized that, "…hostile nations are probing in the computer networks for ways to spark chaos if war should break out."[3] However, it is not only unauthorized access to networks that must be protected against, but authorized users of the secure communications systems can knowingly (malicious) or unknowingly exploit the vulnerabilities of these information systems.

Throughout the 1990s, the United States military forces have attempted to leverage technology to offset the dramatic decline in both the defense budget and personnel force strength. Research conducted by Colonel Gordon Ward supports this idea of leveraging technology, as he found that:

> …as militaries downsize due to political pressures brought about by reduced budgets, it is expected that advanced technology will be necessary to increase the effectiveness of the smaller forces. The military views technology as the enabler to achieve a more flexible response with fewer soldiers.[4]

As a visionary for the use of advances in information technology, Colonel Ward goes on to succinctly state that:

> Using integrated sensors, communications, and data fusion systems planners will access and process, in near-real time, critical campaign information, enabling

[1] McCann, Carol and Ross Pigeau, The Human in Command: Exploring the Modern Military Experience (New York, New York: Kluwer Academic/Plenum Publishers, 2000), 1.

[2] Campen, Alan D. and Douglas H. Dearth, Cyberwar 3.0: Human Factors in Information Operations and Future Conflict (Fairfax, Virginia: AFCEA International Press, 2000), 15-16.

[3] de Borchgrave, Arnaud et al, Cyber Threats and Information Security: Meeting the 21st Century Challenge (Washington, D.C., The CSIS Press, 2001), XI.

[4] Ward, Gordon D., 21st Century Technology – Achilles' Heel of Military Commanders! (Toronto, Canadian Forces College, 2001), 18.

> them to retarget, redirect, or reengage their forces in a timely and opportunistic fashion.[5]

In response to decreased defense budgets, the United States Air Force has turned to advanced technology to support a 'faster, better, cheaper' attitude while striving to create the 'light, lean, and lethal' combat force for the 21st Century.

Although the United States Air Force budget and personnel cuts occurred across the board, the communications and information career field took an exceptionally hard hit. Unfortunately, these programmed cutbacks took place while the global economy was booming and information technology (IT) personnel were in high demand. Thus, it was easy for companies to recruit many well-trained and experienced IT personnel away from the military, with money and benefits that the United States military could not match. This author has observed that in order for the United States military to meet the challenge of creating 'faster, better, cheaper' secure communications systems, the United States military focused its efforts on integrating communications applications and fusing data from single service stove-piped communications systems onto a single joint system of systems where the data could be shared by authorized users. Hence, the United States has focused on the development of the Global Command and Control System (GCCS). In the fall of 1996, the GCCS became the Department of Defense's "computerized system of record for strategic command and control functions."[6] With a vast array of integrated communications capabilities, the GCCS is a key force enabler that provides commanders at all levels of planning (strategic, operational, and tactical) with real-time situational awareness. The GCCS can facilitate critical decision-making for commanders to react and execute military actions when time is of the essence.[7] However, this streamlining effort to focus on integrating several software applications onto one secure communications platform does not come without costs.

This essay will argue that human factors must be considered during the integration of advanced technology into command and control systems. It will begin with defining terms such as human factors, integration and a brief introduction of command and control to provide the framework for communications systems analysis. It will then describe external (unauthorized

[5] Ward, Gordon D., 21st Century Technology – Achilles' Heel of Military Commanders! (Toronto, Canadian Forces College, 2001), 17.

[6] Defense Information Systems Agency, "The Global Command and Control System (GCCS)," (online), accessed 4 March 2003; available from http://gccs.disa.mil/gccs/.

[7] Ibid.

access) and internal (authorized user) vulnerabilities that are inherent in communications systems and possible solutions to those vulnerabilities. Finally, it will use the United States Air Force's version of the Global Command and Control System as a case study to illustrate the importance of human factors when developing potentially complex communications systems.

To set the stage for analysis, a working definition of human factors is required. For the purposes of this essay, human factors relate to motivators and attitudes towards information systems. In other words, how humans interface with communications systems will determine the overall effectiveness and reliability of that information system as a force enabler.

As for integration, this essay will use the term integration in referring to the bringing together of several information system applications so that the raw data can be shared in a computing environment that limits redundancies. This raw data can be used by the information system applications to aid the decision-making process for commanders at every level, throughout the theater of operations.

Volumes of resources provide definitions of command and control. While several variances exist for what command is, for the purposes of this essay, it is the ability for a commander to continue to adeptly focus on the broader context of a situation and make the right decision for execution with whatever information might be available.[8] Commanders regularly make critical decisions based on the facts and information they have available at the time of their decision. To assist commanders in the decision-making process, organizations often look to information technology for solutions. However, the key to successfully finding a technological solution to facilitate decision-making often involves the requirement to filter out an overwhelming amount of data to provide clear, succinct bits of information that is truly useful for commanders. Unfortunately, the technical solutions to fulfill communications requirements are not always as simple to use, as commanders might prefer them to be. Sean Edwards of RAND emphasizes the point that:

> …the goal of information superiority will require unprecedented amounts of information to be made available to soldiers. Key questions remain, particularly with regard to data type, quality, destination, and timeliness. Communication systems must be managed as a scarce physical resource. Many experts are working to find the right balance between information supply and demand for

[8] McCann, Carol and Ross Pigeau, The Human in Command: Exploring the Modern Military Experience (New York, New York: Kluwer Academic/Plenum Publishers, 2000), 11.

> various command echelons. Too much information can lead to overload, and too little information would preclude optimum use of emerging technologies.[9]

Commanders constantly look for that edge in information superiority, to assist in their situational awareness and to help them make sound command decisions.

Today, commanders have come to depend on robust communications systems that provide them with sufficient information and intelligence to help clear the fog of war. Certainly, a robust communications system is relative to the effectiveness of the information gained by its use. A case in point can be found in Rwanda. In this country, the standard of living has not developed on par with the standards of more modern western countries. Generally, Rwanda's civil and telecommunications infrastructure is poorly developed, but the basic radio has been used to relay the "…voice of authority, with a status that made it a powerful tool for disseminating information, misinformation, and propaganda, as well as for overall control of the masses."[10] This illustration of the basic radio supports the importance of the human factor and command and control systems. Of all the tools that advanced technology provides for command, Brigadier General (Retired) Stanley Cherrie observed:

> One of the first documents I came across in reviewing the topic of command was the August 1995 issue of *Military Review*, the U.S. Army's professional journal. Its cover depicts the command decision-making process supported by an entire panoply of technology: crewless aerial vehicles linked by satellite to the commander's suite of digital command and control devices, Joint Surveillance Target Acquisition Radar feeds converging in the same suite, and individual vehicles deployed with their own situational awareness consoles. But all this technology would be useless without the person in the centre of the picture: a battle-hardened senior commander, who will, in the end, be called upon to make a decision. I could not have designed a better way to illustrate my position that the human is the most important element in command.[11]

Let us now turn our attention to an aspect that goes hand-in-hand with command; control. For the purposes of this essay control is, "That authority exercised by a commander over part of the activities of subordinate organizations, or other organizations not normally under his

[9] Sean J.A. Edwards, Freeing Mercury's Wings: Improving Tactical Communications in Cities (Santa Monica, California: RAND, 2001), 9-10.
[10] McCann, Carol and Ross Pigeau, The Human in Command: Exploring the Modern Military Experience (New York, New York: Kluwer Academic/Plenum Publishers, 2000), 33.
[11] Ibid., 18.

command, which encompasses the responsibility for implementing orders or directives." (NATO, 1988)[12] Taken together in a combined perspective, command and control is:

> The exercise of authority and direction by a designated commander over assigned forces in the accomplishment of the force's mission. The functions of command and control are performed through an arrangement of personnel, equipment, communications, facilities and procedures which are employed by a commander in planning, directing, co-ordinating and controlling forces in the accomplishment of his mission. (NATO, 1988)[13]

This is essentially at the heart of the United States' Global Command and Control System. This essay refers to a command and control system as an information system that is used as a tool by commanders to carry out their responsibilities in providing direction in their organizations. General Cherrie's observation further illustrates the true center of importance when it comes to command and control systems. Unfortunately, as commanders focus their efforts on leveraging technology to increase the capabilities of their command and control systems, human factor considerations are almost an afterthought as they rush to field 'new and improved' communications systems.

At one extreme, command and control communications systems can provide an overwhelming amount of information. This was the case during the initial months of the 1991 Gulf War, which led to information overload until the information was filtered and focused. Initially, war planners were overwhelmed by the amount of raw data that poured over the communications systems. However, at the other extreme, the available communications systems may not be robust enough to provide enough decisive information for the commander. In either case, "…commanders must be able to think clearly, based on experience, and make those "gut feel" decisions calmly and accurately, when necessary."[14] The Global Command and Control System is an evolving communications system designed to facilitate a commanders' situational awareness on the battlefield. However, as Lieutenant-General R.R. Crabbe points out, there are drawbacks to what a strategic, operational, and tactical commander can see or should be able to see. General Crabbe noted that:

> …we are now seeing – a proliferation of information systems and information available to commanders. Commanders have immediate access to their bosses

[12] McCann, Carol and Ross Pigeau, The Human in Command: Exploring the Modern Military Experience (New York, New York: Kluwer Academic/Plenum Publishers, 2000), 165.
[13] Ibid., 165.
[14] Ibid., 12.

> and their bosses' bosses. Intelligence from all sources can be fed in and analyzed very quickly by an intelligence centre. This continual barrage of information and intelligence can and will influence command.[15]

Indeed, with commander concerns of situational awareness, the lines of command are blurring as strategic and operational commanders are tempted to make tactical-level decisions because of the information that they have available. The Global Command and Control System focuses in large part on enabling commanders to effectively control their forces and resources. By integrating stove-piped legacy communications systems into one system, the United States' Global Command and Control System will provide one access point, one communications system, for commanders to exercise control.

With some background on what command and control are, and how communications systems facilitate these functions, one must also be cognizant of the threats and vulnerabilities of these force-enabling systems. While human factors are the focus of this essay, other communications system vulnerabilities include atmospheric or environmental effects. For example, in 1998, a solar flare that occurred millions of miles from Earth, cut off cellular phone services to 4 million users for several hours.[16] Incidents like this could have detrimental effects on military command and control information systems since 95% of the information traversing military communications networks depend on the integrity of commercial network infrastructure.[17]

However, unlike distant solar flares, the more controllable human factor threats to military command and control systems must be considered during the budgeting and technical development of the system. According to Dr. Michael McNamara of the National Defense University, "The reason for this is simple: any system or technology designed by humans can also be broken by that same human ingenuity. Humans are complex and adaptive organisms and, if properly inspired, will discover creative ways to circumvent security measures."[18] Experience and observations on information systems leads the author to similar views about

[15] McCann, Carol and Ross Pigeau, The Human in Command: Exploring the Modern Military Experience (New York, New York: Kluwer Academic/Plenum Publishers, 2000), 15.
[16] Ward, Gordon D., 21st Century Technology – Achilles' Heel of Military Commanders! (Toronto, Canadian Forces College, 2001), 16.
[17] Ibid., 15.
[18] Campen, Alan D. and Douglas H. Dearth, Cyberwar 3.0: Human Factors in Information Operations and Future Conflict (Fairfax, Virginia: AFCEA International Press, 2000), 78.

human behavior. Armed with time and the proper tools, any information system that connects globally to the Internet is vulnerable to human threats.

> ***In the context of the 21st Century Information Warfare the highest realization of warfare is to attack the information (data, plans, program, etc.) required for the execution of the adversary's strategy by whatever means – including direct information attack.***[19]

Whereas extensive training is required to operate high technology weapons systems, with minimal instruction, a computer can be used by almost anyone.[20] Global communications systems can benefit anyone who knows how to take advantage of the systems. Commercial industries have taken the lead in developing robust communications technology. In fact, commercial information technology and infrastructure has been adopted for military use to out-think and out-maneuver adversaries on the battlefield.[21] Militaries around the world know that information superiority can provide decisive real-time sensor-to-shooter battlespace awareness to warfighters in the 21st century.[22] However, just as easily as military and civilian organizations reap the benefits of global connectivity, terrorist organizations, such as the al-Qaida network, can leverage that same technology to direct or conduct global attacks, physically or simply by cyber warfare, without requiring a centrally located command center.[23]

As information technology advances, so too does the reliance on that technology. Human factors have a direct impact on the application of that technology, both good and bad. Dr. McNamara stresses:

> Our increasing reliance upon this technology has simultaneously created a myriad of vulnerabilities that threaten these same advancements. The search for solutions must incorporate an increased awareness of the human behavioral dimension of this complex problem. While the information environment has introduced a new

[19] Campen, Alan D. and Douglas H. Dearth, Cyberwar 3.0: Human Factors in Information Operations and Future Conflict (Fairfax, Virginia: AFCEA International Press, 2000), 44.
[20] Ibid., 11.
[21] Sean J.A. Edwards, Freeing Mercury's Wings: Improving Tactical Communications in Cities (Santa Monica, California: RAND, 2001), 2-3.
[22] Ward, Gordon D., 21st Century Technology – Achilles' Heel of Military Commanders! (Toronto, Canadian Forces College, 2001), 12.
[23] de Borchgrave, Arnaud et al, Cyber Threats and Information Security: Meeting the 21st Century Challenge (Washington, D.C., The CSIS Press, 2001), X.

> set of problems, the issue is not with the technology but the human use and misuse of that technology.[24]

To combat human factor vulnerabilities to information systems, information security specialists have developed physical security measures to mitigate some of the risks to protect the systems.[25] Unfortunately in the communications technology industry, security of the systems is both expensive and often not thought about until a system is fielded.[26] Michael Vatis, former director of the FBI's National Infrastructure Protection Center (NIPC) and the nation's top cyber cop, at the World E-Commerce Forum in London in October 2000 stated, "We have seen a rush of products to the market with new features, and security is usually an afterthought."[27] This afterthought for communications system security is not only an afterthought for commercial systems, but it occurs with military systems as well. In the Pacific theater, the author's experience in 2002 has witnessed million dollar communications applications being pulled offline because their use on the military network opened huge technical vulnerabilities that were beyond risk tolerance. Certainly these cases occurred because the application developers were unaware of the capabilities afforded to external human threats to the system.

The Department of Defense (DoD) is all too aware of the external (unauthorized access) threats to its communications systems. Examples of human injected external threats to communications systems come in many forms, but include computer codes such as, "Worms, viruses, Trojan horses, logic bombs, trap doors, denial-of-service (DOS) attacks, and malicious code…."[28] Any one of these threats could be exploited by adversaries in an attempt to gain the strategic advantage on the battlefield.[29] However, one of the easiest exploitable vulnerabilities is the DOS attack because of bandwidth limitations, causing information processing slowdowns or complete loss of connectivity.

> A classic DOS attack involves overwhelming the available bandwidth, "by "spamming" an unclassified network with self-replicating message traffic, the nodes would become congested with packages of useless data, causing the network to crash or at least slowdown creating backlogs for official traffic. The

[24] Campen, Alan D. and Douglas H. Dearth, Cyberwar 3.0: Human Factors in Information Operations and Future Conflict (Fairfax, Virginia: AFCEA International Press, 2000), 77.
[25] Ibid., 78.
[26] Ibid., 77.
[27] de Borchgrave, Arnaud et al, Cyber Threats and Information Security: Meeting the 21st Century Challenge (Washington, D.C., The CSIS Press, 2001), XI.
[28] Ibid., X.
[29] Ibid., X.

> resulting denial of services could likely affect classified systems as well because they typically use the same communications backbone, except the data is encrypted. For a smaller military force, there is a disproportionately greater return on investment if they can bring down a technologically reliant nation.[30]

Additionally, compounding the complexity of enormous job for information security specialists is the fact that several thousands of Internet sites provide details of 'how to' instructions for exploiting computer network vulnerabilities.[31]

Some of the DoD's countermeasures to external threats include creating an electronic barrier or firewall between the non-DoD communications systems and the DoD communications systems. Firewalls are effective gates for information as long as the network administrator knows what firewall ports or access points are authorized for use. During the mid-1990s when firewalls were initially approved for use in the DoD, some network administrators successfully installed the firewall, only to leave the default settings in place. In other words, a true electronic barrier was not in place until the factory settings were removed and replaced by the DoD settings.

Headlines of communications service interruptions usually focus on external causes, either by hacker or environmental reasons. However, a potentially more harmful threat to communications systems comes from internal sources, or authorized users of the system. In the case of a hacker, he may not realize the implications associated with his successful access onto a system.[32] Such was the case in the movie *War Games* where the main character broke into the missile launch mainframe computer while looking for computer games. The hacker risks detection while browsing through the system for potential targets.[33] On the other hand, an authorized user of the system can use their trusted-user access to browse, capture, or worse yet sabotage or destroy data, all with little risk of detection.[34]

Richard Clarke, the National Coordinator for Security, Infrastructure Protection and Counter-Terrorism, uses the analogy of defending against insider threats to communications systems by questioning the purpose of calling more police to respond to unlawful entry into open

[30] Ward, Gordon D., 21st Century Technology – Achilles' Heel of Military Commanders! (Toronto, Canadian Forces College, 2001), 16.

[31] de Borchgrave, Arnaud et al, Cyber Threats and Information Security: Meeting the 21st Century Challenge (Washington, D.C., The CSIS Press, 2001), X.

[32] Campen, Alan D. and Douglas H. Dearth, Cyberwar 3.0: Human Factors in Information Operations and Future Conflict (Fairfax, Virginia: AFCEA International Press, 2000), 79.

[33] Ibid., 79.

[34] Ibid., 79.

doors.[35] This is a very telling analogy with an all too truthful insight that even if there are locks on the doors, all of the insiders have the right keys to gain legitimate access.[36]

The insider threat to computer networks is real and a growing problem. A 1999 Computer Security Institute/FBI reported that:

> …55 percent of respondents reported malicious activities by insiders. The 2000 version of this same report puts that figure at 71 percent. Is the problem growing, or are we just getting better at detecting it? Whatever the answer, this data indicates that the probability on insider risk activity is clearly high, and their knowledge of the system increases the likelihood of serious damage.[37]

Indeed, insiders are authorized access to many areas of their communications systems. Dr. McNamara reiterates that once access is gained to the inside of a network, the trusted-user can seek out system vulnerabilities for future exploitation.[38]

So what is the solution to defending communications systems from insider vulnerabilities? The number one way to defend against it is computer security education. However, the response to insider malicious activity is usually "reactive" and handled discretely to prevent other workers from the same exploitation. In other words, a prevention educational opportunity is missed.[39] Organizations can learn from scientific studies that point out the root causes of the reasons behind human behavior and attack prevention from that angle.[40] Some of the known reasons for insider hacking include things such as boredom at work, the thrill of discovering system vulnerabilities,[41] money, and maliciousness for being overworked[42] or receiving low ratings on a report. In his research of human factors that prevent criminal behavior, Dr. McNamara found that a strong social structure decreased the likelihood that a person would take part in activities that would reflect negatively upon them.[43] Dr. McNamara goes on to emphasize that:

> The best security technologies and products cannot compensate for the lack of a coherent security policy or architecture. While necessary, auditing, monitoring

[35] Campen, Alan D. and Douglas H. Dearth, Cyberwar 3.0: Human Factors in Information Operations and Future Conflict (Fairfax, Virginia: AFCEA International Press, 2000), 77.
[36] Ibid., 77.
[37] Ibid., 79.
[38] Ibid., 79.
[39] Ibid., 80.
[40] Ibid., 84.
[41] Ibid., 82.
[42] Ibid., 84.
[43] Ibid., 81.

> and investigations are very costly reactive efforts. If properly engineered and implemented, security awareness and training efforts can seek to prevent or mitigate the occurrence of problems caused by the insider threat to information systems before the damage is done.[44]

Again, the cheapest and easiest countermeasure to the insider threat is a strong organizational foundation in information security education. Armed with a broad overview of the enabling capabilities of communications systems, as well as some of their vulnerabilities and counteractions to those vulnerabilities, let us turn to a practical application of this information.

The United States DoD's enormous reliance upon computer systems and computer technology in 2001 equated to, "…roughly 10,000 computer systems – 2,000 of which are "mission-critical" – and 1.5 million computers."[45] However, the main focus of military commanders is to develop a complex communications system to assure battlespace information superiority and real-time situational awareness.[46] This complex communications system would incorporate both land and aerial sensors to develop a detailed picture of the battlespace, and allow friendly forces to take the initiative in combat operations before the enemy can detect and respond.[47] In essence, the advances in the communications technology have compressed the observe, orient, decide and act (OODA) cycle.[48] This is only one of the many evolving capabilities of the Global Command and Control System in the United States Air Force (GCCS-AF). Graphically displayed below is the evolving integration of specific communications applications that have migrated onto the GCCS.

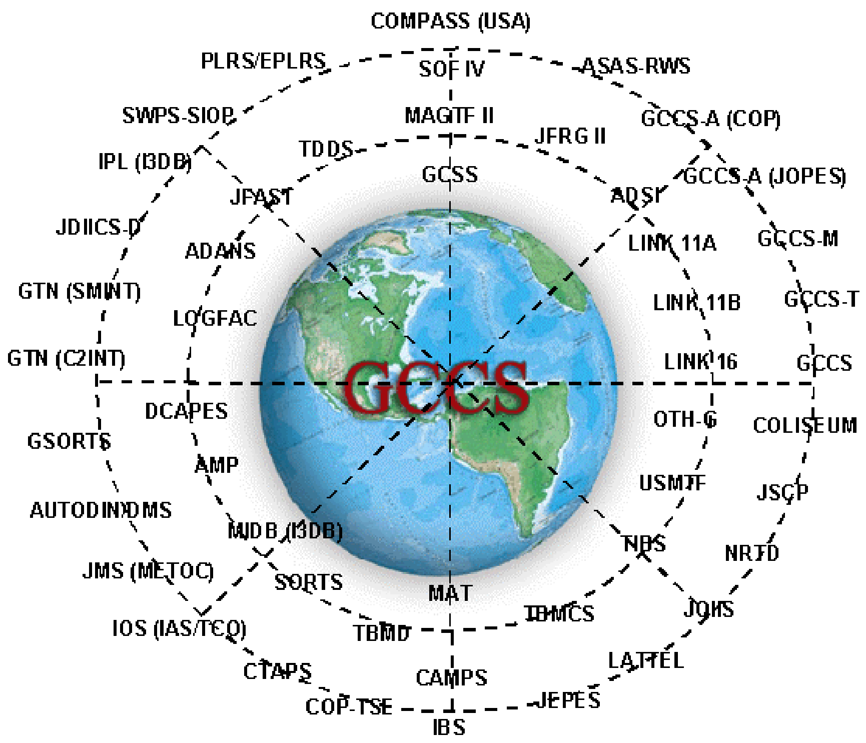
[44] Campen, Alan D. and Douglas H. Dearth, Cyberwar 3.0: Human Factors in Information Operations and Future Conflict (Fairfax, Virginia: AFCEA International Press, 2000), 83.

[45] de Borchgrave, Arnaud et al, Cyber Threats and Information Security: Meeting the 21st Century Challenge (Washington, D.C., The CSIS Press, 2001), XI.

[46] Sean J.A. Edwards, Freeing Mercury's Wings: Improving Tactical Communications in Cities (Santa Monica, California: RAND, 2001), 5.

[47] Ward, Gordon D., 21st Century Technology – Achilles' Heel of Military Commanders! (Toronto, Canadian Forces College, 2001), 8.

[48] Ibid., 7.



[49]

What is the DoD's GCCS? It is the evolving joint command and control system that is continually growing as it incorporates more automated tools to support operational planners and decision makers in the United States military forces and their allies. The United States Air Force's version of this system has specific software segments loaded to support Air Force-specific functions such as air planning and air movement logistics and tracking. For the warfighter, GCCS provides access to the Air Tasking Order (ATO), which delineates the order of battle in the air. Additionally, GCCS provides situational awareness for the warfighter, through the Common Operational Picture (COP). The COP graphically displays various data inputs that are received from various ground and space-based sensors, into a real-time battle picture.[50]

The GCCS is centrally managed by the Electronic Systems Center (ESC) where all software integration and testing occurs. Information security plays an important role in every military operation and the U.S. military has tested and developed specific secure communications systems to ensure the integrity of our decision-making information. In addition

[49] Defense Information Systems Agency, "The Global Command and Control System (GCCS)," (online), accessed 29 January 2003; available from http://gccs.disa.mil/gccs/.
[50] United States Department of Defense, "Global Command and Control System Adopted," (online), accessed 29 January 2003; available from http://www.defenselink.mil/news/Sep1996/b092696_bt552-96.html.

to ensuring the GCCS complies with a tightly controlled standard system configuration, part of ESC's focus is to enable GCCS to provide critical real-time information to key decision-makers.[51] The Air Force Command and Control, Intelligence, Surveillance, and Reconnaissance Center (AFC2ISRC) is the focal point for United States Air Force users. Following Moore's Law which "predicts a doubling in semiconductor processing power, or circuit density, every 18 months,"[52] one-third of the GCCS-AF workstations are replaced annually to keep up with advances in commercial-off-the-shelf (COTS) technology. Amazingly enough, GCCS-AF is still only an early phase of a larger, more ambitious effort known as C4I (Command, Control, Communications, Computers, and Intelligence) for the Warrior. The C4I for the Warrior vision is to fuse all command, control, communications and intelligence nodes into a seamless interoperable command and control system between each of the U.S. military services. The development and evolution of the GCCS is a critical step in making this vision into a reality.[53]

What are some of the limitations of GCCS-AF? High on the list of GCCS-AF limitations includes complexity of use and processing speed. Keeping the human dimension in m information system that is used during military operations. Therefore, communications bandwidth remains a critical limiting factor on the use of technology to support information superiority. GCCS-AF can provide critical situational awareness capabilities to commanders at all levels, however, the United States Army and intelligence requirements take up the lion's share of the available communications pipe. The easy solution for maintaining the processing speed of GCCS-AF is to deploy an application server and a COP server with the GCCS-AF workstations. It is much faster to pull a small stream of data over a small communications pipe than it is to pull huge software application files across the same pipe. Essentially, minor adjustments to tactics, techniques, and procedures (TTPs) would be a simple and cheap solution to data stream congestion over limited bandwidth communications circuits.[55] The bottom line is that training, system evolution, and TTPs all involve human interaction with the system to overcome major limiting factors.

With an appreciation of the two greatest limitations of GCCS-AF, complexity of use and bandwidth, and possible solutions to those limitations, one should look at potentially inherent vulnerabilities to GCCS-AF. As GCCS-AF develops into a system of systems, potential system vulnerabilities must be mitigated before they can be exploited. System developers have taken the first step of mitigating system vulnerabilities by integrating GCCS-AF onto the U.S. military classified network, or the SIPRNet. The SIPRNet involves a complex communications infrastructure that includes such things as state-of-the-art encryption devices, alarmed conduit, and very restrictive firewall protection, before sending information packets over the global Internet backbone. All of the security measures incorporated in the SIPRNet are transparent to GCCS-AF users. However, in this case as with other information systems, it is the GCCS-AF users that are the number one vulnerability to the system. All of the authorized user vulnerabilities described earlier also apply to this command and control system. However, the key to countering this vulnerability is GCCS-AF user security education. By following strict security discipline and procedures, unauthorized access could be virtually be eliminated. Hackers (or unauthorized users) into the system are the second highest GCCS-AF vulnerability concern. Why? Because GCCS-AF is on an encrypted classified command and control network

[54] McCann, Carol and Ross Pigeau, The Human in Command: Exploring the Modern Military Experience (New York, New York: Kluwer Academic/Plenum Publishers, 2000), 3.
[55] Sean J.A. Edwards, Freeing Mercury's Wings: Improving Tactical Communications in Cities (Santa Monica, California: RAND, 2001), 3.

and once an unauthorized user gains access to the SIPRNet, the floodgates are opened to all of the data and information on the network; the impact would be enormous. Instead of the United States leveraging technology to get into an adversary's OODA-loop, the adversary could be using that same technology to watch the activities of the United States military planners and decision makers, from their desktops, and plan their military campaigns accordingly. Developers at ESC perform the operations, tests and evaluations on all GCCS equipment to certify the equipment as secure and sustainable before it is connected to the classified network. However, as a word of caution, cyber criminals were able to hack through the firewalls of Microsoft and many Fortune 500 companies. That type of experienced hacker is a threat to the SIPRNet and any information system connected to it.[56] Given enough time, this author is of the opinion that any information system that uses the Internet to transfer electronic information is vulnerable to unauthorized access. As with the GCCS-AF limitations, the GCCS-AF vulnerabilities involve human interactions that can maintain the security of the system, or provide an avenue for information exploitation.

The evolution and technical development of GCCS-AF into a system of systems emphasizes the need for human factor considerations. As much as communications systems users might like plug-and-play aspects of unclassified information systems, GCCS-AF provides a clear example of limitations and vulnerabilities that can be addressed by simply considering the humans who will be using the system as well as the humans who might attempt to exploit the system. This essay put forth the argument that human factors must be considered during the integration of advanced technology into command and control systems.

In response to a declining defense budget and cutbacks in personnel, the United States focused on streamlining activities that leveraged technology to support a 'light, lean, and lethal' military force. This essay began with a brief introduction of command and control to provide the framework for communications systems analysis. GCCS-AF is truly a system of systems that incorporates many automated support tools for military support and command and control functions. In continuing its focus on the human dimension, the essay then described external (unauthorized access) and internal (authorized user) vulnerabilities that are inherent in communications systems and possible solutions to those vulnerabilities. As noted, GCCS-AF is

[56] de Borchgrave, Arnaud et al, Cyber Threats and Information Security: Meeting the 21st Century Challenge (Washington, D.C., The CSIS Press, 2001), XIII.

not immune to those vulnerabilities that plague the information technology industry. However, security of the system is paramount and meticulous testing is performed by ESC with respect to both equipment and software development. Throughout this essay, the author used the common theme of human factor considerations to develop the thesis argument.

The United States DoD and other militaries around the world may be able to save billions of dollars in m

WORK CITED

Alberts, David S., The Unintended Consequences of Information Age Technologies, Washington, DC: The Institute for National Strategic Studies, 1996.

Anderson, Robert H. et al., Securing the U.S. Defense Information Infrastructure: A Proposed Approach, Santa Monica, California: RAND, 1999.

Anon. "The Future of Warfare." The Economist, accessed through http://proquest.umi.com.

Campen, Alan D., The First Information War, Fairfax, Virginia: AFCEA International Press, 1992.

Campen, Alan D. and Douglas H. Dearth, Cyberwar 3.0: Human Factors in Information Operations and Future Conflict, Fairfax, Virginia: AFCEA International Press, 2000.

Darilek, Richard, Measures of Effectiveness for the Information-Age Army, Santa Monica, California: RAND, 2001.

Davis, Paul K. et al., Effects of Terrain, Maneuver Tactics, and C4ISR on the Effectiveness of Long-Range Precision Fires, Santa Monica, California: RAND, 2000.

de Borchgrave, Arnaud et al, Cyber Threats and Information Security: Meeting the 21st Century Challenge, Washington, D.C.: The CSIS Press, 2001.

Defense Information Systems Agency, "The Global Command and Control System (GCCS)," accessed at http://gccs.disa.mil/gccs/.

Edwards, Sean J.A., Freeing Mercury's Wings: Improving Tactical Communications in Cities, Santa Monica, California: RAND, 2001.

Frater, Michael and Michael Ryan, Communications Electronic Warfare and the Digitized Battlefield, Duntroon, Australia: The Land Warfare Studies Centre, 2001.

Grange, MajGen David L. and Col James A. Kelley, "Information Operations for the Ground Commander," Military Review, accessed through http://proquest.umi.com.

Hura, Myron et al., Enhancing Dynamic Command and Control of Air Operations Against Time Critical Targets, Santa Monica, California: RAND, 2002.

Jensen, Richard M., Program on Information Resources Policy, Cambridge, Massachusetts: Program on Information Resources Policy, 1997.

Johansen, Grant A., The ABCA Programme: Rhetoric to Reality, United Kingdom: The Strategic and Combat Studies Institute, 2002.

Latham, Andrew, Understanding the RMA: Braudelian Insights into the Transformation of Warfare, Switzerland: Programme for Strategic and International Security, 1999.

Libicki, Martin, Who Runs What in the Global Information Grid: ways to share local and global responsibility, Santa Monica, California: RAND, 2000.

Lockwood, Jonathan S., "Space Control Versus Space Denial in 21st Century Warfare: Achilles' Heel of the RMA?," Defense & Foreign Affairs Strategic Policy, accessed through http://proquest.umi.com.

McCann, Carol and Ross Pigeau, The Human in Command: Exploring the Modern Military Experience, New York, New York: Kluwer Academic/Plenum Publishers, 2000.

Potts, David, The Big Issue: Command and Combat in the Information Age, United Kingdom: The Strategic and Combat Studies Institute, 2002.

Sharpe, G.E. and Allan English, Principles for Change in the Post-Cold War Command and Control of the Canadian Forces, Winnipeg: Canadian Forces Training Materiel Production Centre, 2002.

Sheffield, Gary and Geoffrey Till, Challenges of High Command in the Twentieth Century, United Kingdom: The Strategic and Combat Studies Institute, 1999.

Simpson, Roy L., "Eyeing IT Trends and Challenges," Nursing Management (Dec 2002).

Sokolski, Henry, "America Helped Arm China. Now What?," The Wall Street Journal, accessed through http://proquest.umi.com.

Tilford, Earl H., Jr., The Revolution in Military Affairs: Prospects and Cautions, Carlisle Barracks, PA: Strategic Studies Institute, 1995.

United States Department of Defense, "Global Command and Control System Adopted," accessed at http://www.defenselink.mil/news/Sep1996/b092696_bt552-96.html.

Waltz, Edward, Information Warfare: Principles and Operations, Norwood, Massachusetts: Artech House, Inc., 1998.

Ward, Gordon D., 21st Century Technology – Achilles' Heel of Military Commanders!, Toronto, Canada, Canadian Forces College, 2001.