REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
04/28/2017	Master's Thesis	SEP 2016-APR 2017

4. TITLE AND SUBTITLE
Efficient Satellite Bandwidth Management of Tactical Satellite Systems

5a. CONTRACT NUMBER
N/A

5b. GRANT NUMBER
N/A

5c. PROGRAM ELEMENT NUMBER
N/A

6. AUTHOR(S)
Young, Peter J. Major USMC

5d. PROJECT NUMBER
N/A

5e. TASK NUMBER
N/A

5f. WORK UNIT NUMBER
N/A

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
USMC Command and Staff College
Marine Corps University
2076 South Street
Quantico, VA 22134-5068

8. PERFORMING ORGANIZATION REPORT NUMBER
N/A

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
N/A

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT
The demand for tactical satellite bandwidth will continue to increase because of a lack of knowledge concerning the makeup and behavior of Programs of Record (POR) and commonly accessed websites. A well run, prioritized, and monitored network will be able to run the appropriate programs to complete the unit's mission if the planners have an understanding of the network behavior of required applications. Tactical satellites networks have latency and bandwidth rates that negatively affect network performance. With the Marine Operating Concept, it becomes imperative available bandwidth is properly utilized to accomplish the units' mission.

15. SUBJECT TERMS
Satellite Communications, Network Monitoring, cyber,

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			USMC Command and Staff College
					19b. TELEPHONE NUMBER *(Include area code)*
Unclass	Unclass	Unclass	UU	42	(703) 784-3330 (Admin Office)

United States Marine Corps
Command and Staff College
Marine Corps University
2076 South Street
Marine Corps Combat Development Command
Quantico, Virginia 22134-5068

MASTER OF MILITARY STUDIES

TITLE:
Efficient Satellite Bandwidth Management of Tactical Satellite Systems

SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF MILITARY STUDIES

AUTHOR:

Peter J Young
Major, USMC

AY 16-17

Mentor and Oral Defense Committee Member: Flynn, M.
Approved:
Date: 4/27/17

Oral Defense Committee Member: J.W. Gordon
Approved:
Date: 4/27/17

United States Marine Corps
Command and Staff College
Marine Corps University
2076 South Street
Marine Corps Combat Development Command
Quantico, Virginia 22134-5068

MASTER OF MILITARY STUDIES

TITLE:
Efficient Satellite Bandwidth Management of Tactical Satellite Systems

SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF MILITARY STUDIES

AUTHOR:

Peter J Young
Major, USMC

AY 16-17

Mentor and Oral Defense Committee Member: _____
Approved: _____
Date: _____

Oral Defense Committee Member: _____
Approved: _____
Date: _____

Executive Summary

Title: The Efficient Satellite Bandwidth Management of Tactical Satellite Systems

Author: Major Peter J. Young, United States Marine Corps

Thesis: The demand for tactical satellite bandwidth will continue to increase because of a lack of knowledge concerning the makeup and behavior of Programs of Record (POR) and commonly accessed websites. A well run, prioritized, and monitored network will be able to run the appropriate programs to complete the unit's mission if the planners have an understanding of the network behavior of required applications.

Discussion: Tactical satellite networks operate with high latency and error rates that create network patterns standard users are not used to in their daily lives. The computer habits a user has in garrison or at home can lead to enormous amounts of Internet traffic which will bring tactical networks to congestive failure. Congestion on a satellite network will quickly frustrate users and, if it is not corrected, can directly impact a unit's ability to complete its mission. As the Marine Corps moves to the future with the new Marine Operating Concept, it becomes more imperative that long distance communication is available and reliable. The current amount of satellite bandwidth will be sufficient to support combat operations if Marines train for minimal connectivity and make decisions before the deployment that some applications, websites, and programs are a requirement for mission accomplishment while others are a convenience.

Conclusion: Many tactical networks become unusable and unreliable because the operators, chiefs, and officers that employ them are not aware of the traffic that is traversing the satellite. When network analysis is employed, improperly configured devices creating unnecessary traffic can be corrected and users browsing non-mission related sites can be restricted. The result is a network supporting only the key applications required to complete the current mission. It is not necessary to block all web browsing because, when used properly, non secure Internet can fill gaps in knowledge and reduce embark space. However, network analysis is a science and art that needs to be taught to the military cyber operators and supervisors.

DISCLAIMER

THE OPINIONS AND CONCLUSIONS EXPRESSED HEREIN ARE THOSE OF THE INDIVIDUAL STUDENT AUTHOR AND DO NOT NECESSARILY REPRESENT THE VIEWS OF EITHER THE MARINE CORPS COMMAND AND STAFF COLLEGE OR ANY OTHER GOVERNMENTAL AGENCY. REFERENCES TO THIS STUDY SHOULD INCLUDE THE FOREGOING STATEMENT.

Table of Contents

Page

I. Introduction

US military tactical satellite systems suffer from limited bandwidth, latency, and jitter at degrees that are not experienced in the commercial networks that the majority of applications were designed for.[1] Standard military users from private to general have become accustomed to high-speed internet in their homes, offices, and mobile devices. The transfer to a highly latent time division multiple access (TDMA)[2] satellite system like the very small aperture (VSAT) family of tactical satellite equipment compounds the time taken to perform the most basic functions across the Wide Area Network (WAN). It is not uncommon to find a user, on a tactical network, conducting mission essential business with several browser tabs open to their social medial profile, sports teams, and news sites. Modern computer users multitask and stay connected. However, a tactical satellite network rarely has sufficient bandwidth to support such habits. Unnecessary Non Secure Internet Protocol Router (NIPR) traffic, such as social media and web browsing, can cripple a network if the local cyber operators are unable to properly monitor WAN traffic.[3] Mission essential software programs must also be planned and configured for satellite networks, or they generate excessive or inefficient traffic that will congest limited bandwidth WAN links. The demand for tactical satellite bandwidth will continue to increase because of a lack of knowledge concerning the makeup and behavior of Programs of Record (POR) and commonly accessed websites. A well run, prioritized, and monitored network will be able to run the appropriate programs to complete the unit's mission if the planners have an understanding of the network behavior of required applications. To maximize the limited satellite bandwidth available to the tactical users, network operators require a more comprehensive understanding their WAN traffic. If given local ability to monitor and shape traffic created by unsecure web browsing, security programs, and Programs of Record,

network managers will give the local commander the ability to choose which traffic is essential for mission accomplishment. Units must learn to operate with minimal amounts of bandwidth by becoming more efficient instead of the spending resources on increasing unrealistic bandwidth requirements. When bandwidth is at a premium, the power to shape your traffic locally will mean the difference between an effective command and control network and a congested, unusable network where web browsing and improperly timed updates cause key systems to fail.[4] As the Marine Operating Concept 2016 and United States Marine Corps Commandant Robert B. Neller have directed, units need to train to operate in low to no communications environments because the Marine Corps may end up in a conflict where bandwidth will be limited or denied.[5] To provide an effective command and control network in a limited bandwidth environment, many garrison luxuries will have to be curtailed, such as social media and NIPR web, to include "essential" web-based services that Marines have become accustomed to, such as Marine Online, Marine Net, Automated Performance Evaluation System, etc. In a combat environment users must be able to operate with only secured networks or radios using text based chat programs as the primary means of data communications.

II. Literature and Source Review

The primary sources on this topic are the joint and Marine Corps doctrine, input from the communications community, and civilian textbooks. The Marine Corps Warfighting Publication 3-40.3, Marine Air Ground Task Force (MAGTF) Communications System describes the Joint Data Network (JDN), NIPRNet, SIPRNet, and Coalition Wide Area Networks and when access would be necessary.[6] The publication also discusses topics of packet switched networks, the preferred method employed by MAGTF Communications networks, and the electromagnetic

spectrum. The problems associated with limited bandwidth are discussed but there are no solutions on how to mitigate them offered up to readers.

The Joint Publication 6-0, Joint Communications Systems, gives a higher level overview on how the electromagnetic spectrum is allocated to provide access to the services and how those services interact to share services.[7] For example, a USMC unit is likely to pull network centric services from an US Army network operations center (NOC). The Joint Publication focuses more on the strategic considerations of service roles and responsibilities.

The Department of Defense (DOD) chief information officer published the Unified Capabilities Master Plan (UC MP) to "define the implementation strategy to converged, net-centric, IP-based enterprise UC."[8] This document gives an understanding on how the whole DOD global information grid, or Defense Information Systems Network (DISN), is employed throughout the globe. It sets guidelines on how products procured by the DOD must comply with guidelines to ensure they can prioritize voice and data traffic while traversing multiple DOD network domains. Any understanding of Marine Corps specific network traffic must be based on how the equipment and programs of record applications comply with the DOD unified capabilities master plan.

The driving guidance behind getting the most of the limited satellite bandwidth available to the Marine Corps comes from the Marine Operating Concept (MOC) and the fragmentary order published by Marine Corps Commandant Robert B. Neller. These documents explain how the Marine Corps plans to remain relevant and a superior fighting force in the future. Near peer competitors can be expected to have technologies that will degrade or eliminate command and control communications links.[9] The Marine Corps, as a whole, is being directed to learn again

the skills of the past where complex operations were conducted without the constant communications links to higher headquarters.

Much of the topics discussed in this paper are based off the experiences of communications officers, chiefs, and network planners that support USMC command and control nodes. An interview was conducted with Major Paulo Alves, who was the lead Marine Expeditionary Forces network planner while deployed in Helmand Providence, Afghanistan in 2011. Major Alves currently works at the Marine Corps Cyberspace Operations Group (MCCOG) the cyber organization that executes Marine Corps and Department of Defense Information Network (DODIN) policies.[10] Also, a white paper published in 2017 by Lieutenant Colonel Atiim Phillips is a recent document from the operating forces that is driving the communications training plans to be in line with the MOC concept of operating in a satellite limited or denied environment. LtCol Phillips is the senior communications officer serving at 3d Marine Expeditionary Brigade on Okinawa Japan. Several articles from communications officers published in the gazette also gave first hand references to complaints and courses of action from the fleet.

III. Tactical Satellite Challenges

Tactical satellite communications creates challenges for planners, operators, and users that do not exist in garrison or commercial networks. Many users have become accustomed to high network performance levels at home and work, and have unrealistic expectations of tactical satellite systems because they are using the same computers, applications, and websites. Satellite bandwidth, in the military, is requested by the communications officer based off the number of users and computers expected to be simultaneously accessing the network. Bandwidth is granted

by the Defense Information Systems Agency satellite network planners based off availability and priority.[11] However, this process is much more complicated than simply calculating the number of users and computers. In the current operating forces, at the battalion or squadron level, it is unlikely more than a Very Small Aperture Terminal-Small (VSAT-S) with a single carrier, providing just over 2 Mbps of bandwidth, will be available. This bandwidth must support secure, non-secure, and coalition networks that contain a multitude of applications required to complete missions and to conduct daily operations.[12] Commercial users focus on one network without satellite links, which makes commercial solutions for tactical satellite networks problematic.

Launching new satellites and adding bandwidth may solve some problems; however, lack of bandwidth is not the only issue that effects data speeds. Even when sufficient bandwidth is available, the network performance across a satellite link is dramatically slower than users are used to. The transmission control protocol (TCP) congestion control algorithms recognize the physical distance travelled by the signal, combined with data loss, as congestion.[13] When a network encounters congestion the sending servers decrease the data rate in an attempt to reduce network traffic to a level that routers can handle. This creates a problem known as the "long fat pipe" problem.[14] When TCP congestion control was designed, most delay was caused by too much traffic which was queued by a router. The protocol was coded to solve this problem by sending less data. So when traffic started being transferred via satellite networks, traffic must traverse to the satellite and back and the delay caused by the speed of light becomes a constant for all traffic. The delay causes TCP to settle at a slower rate despite the availability of more bandwidth.[15] There are programs and devices that can correct this problem, but they can also cause problems when the network becomes congested. This problem is not unique to the military; all satellite users experience a similar problem. However, commercial satellite

providers, such as Hughes Net ™, generally support one household accessing standard Internet services. Most commercial satellite users find online gaming or real time services, voice or video, unusable on these links. Marine Corps tactical VSAT terminals support a host of users using C2 applications, Video Teleconference (VTC), and Voice over Internet Protocol (VoIP) that are less tolerant to the error rates and jitter caused by satellite communications.[16]

To combat the long fat pipe problem, various technologies and equipment have been developed and included into Marine Corps tactical satellite systems. The current family of VSAT systems comes equipped with a TurboIP by Comtech which runs Skipware, a proprietary implementation of Space Communications Protocol Specifications (SCPS).[17] SCPS is an open standard TCP acceleration algorithm designed to reduce the delay caused by latency in the transport of data. The TurboIP also controls the TCP congestion control algorithms and allows data to transfer using the full bandwidth capacity of the satellite link. This ability does not come without a cost. SCPS will allow a single computer to transfer enough data to congest the network. A network running SCPS without proper quality of service can congest itself and make the network unusable. SCPS works well when a few users are accessing the WAN, such as a few users on a commercial satellite. However, when employed by the Marine Corps during tactical operations, multiple servers, users, and C2 applications generate a high number of sessions per machine that the TurboIP cannot handle and network congestion, followed by gridlock, occurs. WAN optimization technology, such as the Comtech Turbo IP, has become a niche technology in the information technology sector and there are several companies that build competing technologies. Modern WAN optimizers have more efficient solutions to the long fat pipe problem and IP accelerator induced congestion. The TurboIP has not been upgraded to the latest

WAN optimization technologies and a technical refresh to the industry standard would allow more efficient usage of available bandwidth.[18]

IV. Network Requirements

Network requirements must be devised based off the units needs, and each unit is unique. A commander has a vision on how they want to command and control and the network must be crafted to suit their needs. These needs can be driven by personal preference as well as mission necessity. For example, a Marine Division relies heavily on classified networks running command and control programs while a Marine Logistics Group focuses on non-secure programs. Currently, in the major subordinate elements' communications offices, there is little knowledge detailing how specific programs act on low bandwidth, high delay, networks. As an example, for years Global Combat Support System-Marine Corps (GCSS-MC) was thought to be unusable on tactical satellite networks because it required more bandwidth than was available on a VSAT. It was later proven that the latency and network congestion was the primary drivers of GCSS-MC failures and once tactics, techniques, and procedures were developed, users began to successfully use the program in deployed environments. Organizations such as Command, Control, Communications, Computers, and Intelligence (C4I), Marine Corps Systems Command (MCSC), and Marine Corps Operational Test and Evaluation Activity (MCOTEA) must do extensive studies on programs of record to provide information on bandwidth consumption and network performance on satellite networks to provide local data planners the information needed to properly apportion and prioritize tactical networks.

Case Study Global Combat Support System-Marine Corps:

GCSS-MC, the current logistics solution employed by the Marine Corps, suffered many setbacks during its roll out. One significant setback was the inability of users on tactical networks to access the enterprise servers while connected via a tactical network. The problem was a consistent complaint at every Operational Advisory Group (OAG) meeting held by the Logistics Command (LOGCOM). When a unit cut over to GCSS-MC, it was unable to conduct maintenance or procure parts without access to GCSS-MC and units devised extensive work around to complete missions while in the field. Users would build large excel documents and transfer them to a garrison remain behind element (RBE) who would spend hours keypunching data. On one deployment, a MEU sacrificed maintenance management personnel to garrison positions because they were unable to complete transactions while afloat. The program and program office suffered serious setbacks as commanders lodged complaints.

When elements of the Program Office and MCSC teamed up to study the problem with extensive network analysis and field visits, the problem was discovered. A combination of computer settings, security conflicts, program behavior, and unexpected network performance led users to believe that the program was inaccessible. There were several computer settings that had to be implemented by the network administrator.[19] However, these non-standard settings were unexpected and even the most experienced administrators could not be expected to know the steps required to get the program to recognize certificates and make secure connection with enterprise. A second, major issue was compatibility with the most up-to-date version of Java. GCSS-MC software development did not keep up with java browser plug-in updates and required users to use an older version. Many security professionals were not aware of GCSS-MC access problems and were, again, unlikely to make the connection. Even with appropriate

knowledge, many would not accept the security risks of using out of date software. The third major obstacle was how GCSS-MC stored java plug-ins on the user's computer. The 13 MB of files were associated with the user's profile on a single computer.[20] On a tactical satellite network, these files were known to take up to an hour to download when first accessing GCSS-MC. Users were not aware of this and would shift to a different computer, resetting the process. Finally, communication with the enterprise servers in Mechanicsburg, Pennsylvania, suffered from an inefficiency that doubled the effects of the latency experienced on satellite networks and would cause the program to appear unresponsive and users would disconnect.

Once the problems were understood, and users were taught how the program operated, users could consistently connect and were able to process transactions at the same speed or faster than on garrison networks. By the time this information was uncovered, GCSS-MC had a bad name and the education process faced an uphill battle. The Program Office developed a communications user's guide and eventually units were taught how to get users online and operating.[21] At this point GCSS-MC is operational on tactical networks as long as a solid satellite network is provided and users understand the unique requirement associated with its implementation. However, communicators and GCSS-MC users continue to blame the system when network congestion is to blame.[22]

Bandwidth Utilization

The volume of websites and applications that are considered 'required' by users on a tactical satellite network is in the hundreds. Appendix A gives a listing of commonly requested programs. These programs have all been determined as "mission essential" by different users.[23] The case study on GCSS-MC shows that not all web-based applications will operate as expected

on a tactical satellite network. Each application listed in Appendix A should get the same deep dive, packet level study given to GCSS-MC. This study would give users and network planners an understanding of how much bandwidth each program utilizes and how that program can be expected to perform in bandwidth congested and restricted environments. Armed with that knowledge, the unit commander determines which applications they will allow on their network when deployed. Currently commanders are basically unaware of the impact of the vast number of "required" programs that the communications unit must provide access to.

Communications officers and data planners should be armed with enough information about programs of record and common website to give a commander the ability to decide which programs are mission essential and which can be eliminated. A data planner, military occupational specialty 0650, is a Warrant Officer MOS employed in the Major Subordinate Command (MSC) level G-6 who is responsible for planning all cyber networks employed by their MSC.[24] When bandwidth is at a premium, a commander needs to decide if a website is worth the cost. The communications community advises the commander, but it is ultimately their decision. They may restrict some "essential" sites, for example, a unit could go to paper morning reports instead of using Marine On-Line (MOL). Eliminating MOL would ensure bandwidth is preserved for what the commander deems more important traffic. Metrics like average data transferred, required updates, and transfer protocols will provide the required information. Another example of inefficient bandwidth allocation is a unit that must operate classified network often chooses to dedicate a satellite link to the classified network instead of tunneling it through a shared network if there are sufficient assets.[25] However, if it is proven that classified applications utilize minimal data, dedicating a 2 Mbps link to the classified network would be a waste. The carrier is paid if it is saturated or not used at all, a properly apportioned

communications plan will be able fully utilize links without creating enough traffic to cause congestion. It is unlikely that a data planner will be able to create this situation without key information on the PoR and commonly accessed sites.

V. Bringing Garrison Practices to the Field

Currently, garrison and tactical networks are completely separate and are managed by different units. A base, post, or station G-6 is normally responsible for all garrison hardware and networks used by the tenant units.[26] However, when the unit transfers to a satellite network, while deployed or on an exercise, the unit's communications section provides the infrastructure. The network performance is significant because of limited bandwidth, latency, and underpowered equipment.[27] Users attempt to conduct business in the field as they would in garrison, which is an unrealistic expectation.

Garrison traffic management

For the USMC garrison units, the current process of blocking unauthorized or unnecessary traffic in garrison involves using a Bluecoat ™ Web Proxy.[28] This device provides a user an ability to see every user connected to the WAN and tracks exactly what sites that user is accessing and the traffic generated by that user. It is a powerful tool and gives state of the art control of the network. However, in garrison the proxy is operated by civilians employed by the local Marine Air-Ground Task Force (MAGTF) Information Technology (IT) Support Center (MITSC) which falls under the base, post, or station G-6. The MITSC is not staffed to closely monitor the volume of traffic and users generated by the tenant units on their network. For instance, the MITSC Western Pacific (Westpac) run the Camp Butler G-6 supports every user on the island of Okinawa, Iwakuni, and most of mainland Japan. During business hours there are

several thousand users connected, with each user accessing dozens of sites simultaneously. The MITSC generally limits their involvement to gross infractions of policy, such as unauthorized content and traffic generation inconsistent with standard users.[29] A user streaming a YouTube video on proper MCMAP procedures can be considered appropriate but a user streaming high definition music videos for eight straight hours is not appropriate, it is unlikely the proxy will discern the difference between the video content. Education of the users and small unit leadership to police appropriate traffic is an appropriate step to cut traffic. However, it is common to find users accessing inappropriate material even though they are being monitored, and offenders are generally the supervisors that are supposed to be policing discipline.

Tactical Traffic Management

On tactical networks, the task of restricting traffic falls on the local 0689, Cyber Security Specialist, which runs the Fortigate ™ firewall. The firewall is a component the information assurance model (IAM) module of the Data Distribution System-Modular (DDSM). The DDSM is the program of record that contains routers, switches, and servers that serve as the tactical data solution for the Marine Corps.[30] The firewall's purpose is to recognize suspicious traffic and block it, to protect the network from attack. It can be used to limit and shape network traffic but it lacks the capabilities of the equipment used in garrison. Also, the Marine tasked with programming and maintenance on the firewall is also responsible for the security of the network. They generally lack the time or knowledge to shape traffic patterns using the firewall, as their focus is security. Programming a firewall to block content consists of crafting a set of rules that must be perfect, or the firewall can become overworked or allow malicious traffic.

When a unit goes to the field they submit a network package for approval and the local commander is granted control over the network while deployed.[31] The commander does not have the training, experience, or time to make network calls on a case by case basis so that responsibility is deferred to the cyber security Marine. These Marines have more tasks to complete than any other cyber operator when deployed, and to task them with programming extensive firewall rules every time a user needs access to a blocked site only adds to their workload. The process of shaping traffic could be offloaded to the 0651 cyber operators, or the 0659 cyber chiefs, who would setup and maintain the network if they were given the appropriate software, hardware, and training required to perform network analysis and traffic shaping.[32] Given this type of control, at the local level, communications officers can make immediate corrections on network offenders and train users on appropriate tactical traffic generation.

Determining Essential Traffic

The question of what sites are necessary still must be answered and the duration of the deployment has as much to do with the answer as the mission of the unit. The mission of the specific unit will dictate specific applications that a commander will deems necessary to complete their mission, to include what morale sites should be allowed. An infantry unit will be concerned with command and control applications, generally operated on secured networks, that give the commander situational awareness of the locations of his units. However, a logistics unit requires access to logistics specific programs such as GCSS-MC, Common Logistics Command and Control (CLC2S), and Battle Command Sustainment Support System (BCS3). These programs are primary logistics programs, required by the Marine Logistics Group (MLG), and are accessed through non-secure networks. It is the job of the units' senior communications officer to discern the needs of the unit and provide access to the required programs. These

programs are necessary for that unit to complete its mission, but once the unit goes tactical a host of other requirements will arise which will be described as mission essential. The volume of military applications and work-related web traffic can overwhelm a low bandwidth satellite network even when morale web sites are blocked.

Garrison Websites Become Mission Critical

If Marines are in the field for an extended period of time, garrison requirements will begin to become mission requirements. Typical problems experienced by most deploying communications units are tactical account access. When the G-6 speaks at any planning meeting they will likely remind users to get their classified, tactical unclassified, and coalition accounts created and activated. However, when the unit arrives in the field a large percentage of users, usually high-ranking staff NCOs and officers, inevitably arrive without accounts. They must submit a System Authorization and Access Request (SAAR), from the field, to legally create an account. The SAAR requires a valid security clearance and up to date cyber awareness training. If the user does not have their training complete they will have to get on MarineNet to complete the training before they will be granted access. Also, the security manager must check their security clearance in the Joint Personnel Adjudication System (JPAS), a web based program. Therefore, MarineNet and JPAS become critical requirements during the first few days of any deployment, when the network is first coming online and devices generate traffic to update and replicate. If the unit is in the field during any required reporting occasions for fitness reports, access to Marine On-Line (MOL) and Automated Performance Evaluation System (APES) will also be critical requirements.[33] Many of these problems could be alleviated with foresight and planning but, inevitably, a high-ranking Marine will require immediate access to these programs and it is unlikely that the communications officer will make them wait until the network is stable.

Another example of the modernization of Marine Corps practices is the electronic morning report. Historically, roll was called and the report given to the commander; however, today all morning reports are done through MOL and even a unit in the field will be expected to submit their morning report if the network is available. This seemingly simple requirement now requires leadership at the platoon level and above to access MOL and submit their morning report daily, causing a spike in traffic. Allowances for tactical users to eliminate the MOL morning report should become standard operating procedure to eliminate this traffic.

VI. Impact of Non-Secure Web Browsing

As soon as a network's Wide Area Network connection is complete, traffic begins to flow as computers, network devices, and servers begin to communicate with their distant end. One of the first sites to be visited on any network is Google, as the cyber Marines begin to test connectivity. Each website visited generates traffic and it all adds up to a congested and unusable network as harmless browsing begins to choke the bandwidth available to conduct command and control. It is not as simple as just telling users to stay off social media. Data can come from computers pulling updates or server replicating, both causing congestion and the local operators have few tools to view network traffic and determine the causes of congestion. An example is a unit that embarks their computers 30 days prior to a deployment and then spends another two weeks in transit and preparation. By the time they begin bringing their computers online those devices have not seen the Web for close to two months and they instantly start to update. If a cyber operator makes a simple error and those computers start pulling updates from Microsoft instead of a local server, the network will quickly become congested. If 100 computers are brought online with the same problem, the network will become unusable until all

updates are received. However, if the operator has a network monitoring tool that shows traffic headed to Microsoft the problem would be solved quickly.

Local Traffic Reduction

"The network is unusable" is a common complaint to cyber operators across the Marine Corps. Many of these operators are unequipped with the tools or the knowledge to do anything about this complaint other than blame the satellite. Running a regiment size unit of users with only a VSAT Small on a 2.4 MSPS carrier, which is approximately ~2.3 Mega bit per second (Mbps), leaves little per user throughput, but it if properly policed it will provide enough access to complete typical missions. The problem arises when users who have access to Gigabit garrison connection speed and 100 Mbps connections at home attempt to surf the web as if they were not in the field. If cyber operators had basic network monitoring skills, they can quickly eliminate high bandwidth users and computers to clear the congestion and get users back online. Cutting social media, rescheduling updates, and reducing large emails are the biggest targets for elimination. Increasing users understanding of the effect of their web habits on the satellite WAN is key to keeping network congestion from hindering mission essential traffic.

Social Media

The fight to eliminate social media from tactical networks is ongoing. The Marine Corps has had multiple policies enacted to reduce social media usage because of bandwidth and operational security concerns. Each time the policy gets relaxed, or not enforced, and eventually the sites are accessible again. The benefits of open internet are improved morale from access to social media, technical answers from web searching, and open source intelligence gathering have outweighed the dangers and social media sites are typically open on most tactical networks.[34]

The operational security concerns of Marines having full access to social media are a different topic, for a different report. However, when social media is allowed on a tactical satellite network the throughput will instantly suffer.[35] Sites like Facebook and YouTube were not designed for bandwidth-constrained environment. Their streaming video, large photos and advertisements generate numerous TCP/IP connections which will utilize all available bandwidth and generate congestion. Congestion will slow connection speeds and impact higher priority traffic.[36] However, social media allows Marines to be connected to their families instantaneously, reducing the uncertainty and homesickness. The modern Marine has grown up with constant connection and has become accustomed to accessing social media on a daily basis. When there is a lull in a deployment or exercise, a chance to get online improves morale and the overall effectiveness of Marines.[37] However, with regards to bandwidth, Facebook is generally the most accessed site on any tactical network. The traffic analysis during a Marine Expeditionary Unit (MEU) deployment showed that over 30 percent of traffic was Facebook alone. When delivering a report on shipboard network activates to PMW 160, there was a notable increase in bandwidth utilization at the same time every day. It was assumed that an update, download, or some ship activity was the cause. However, the ship had instituted "gator hours" where social media was blocked. The daily spike occurred when the hours ended and Facebook was opened up.[38]

Cellular phone usage in a tactical environment would alleviate social media access from the tactical network. However, the constant presence of cellular devices represents a significant threat in a combat environment. Electronic Warfare platforms can track the electromagnetic signature of several hundred phones running Global Positioning software, voice, and data

services. Also, many of the environments where Marines operate, on land and sea, have little to no cellular coverage so users default to their tactical network.

Users circumventing Security/Traffic Shaping

Users will go to great lengths to find work-arounds when sites are blocked, from simple to complex hacks; a determined user can find a way. This problem causes excess work for security professionals, who waste time blocking sites to reduce traffic. For example, in the Navy ADNS quality of service structure, secure hyper text transfer protocol (HTTPS) is prioritized in a higher queue than standard HTTP traffic. This was not general knowledge to shipboard users, but they did notice that if they went to http://www.google.com, they had better success rate then when visiting https://www.google.com. In addition, more savvy users find complex web redirect sites that work around firewalls. When caught, these users are subject to network restrictions and possible punishment, depending on the sites visited. The Cyber Defense Operator is employed to keep the network safe, not spend their time tracking down insiders. However, these same insiders could represent a critical vulnerability if their intentions were espionage as opposed to viewing restricted websites.

Benefits of NIPR access at operator level

Spending hours scrolling through paper publications to find an obscure reference has been eliminated by the web search and online publications library. Search engines are a power solution for many Military Occupational Specialty (MOS), from Cyber to Mechanics, are accustomed to having this information available when troubleshooting a difficult problem. A quick search of the public Internet and restricted DOD sites will give a user access to virtually every technical manual and doctrinal publication needed to solve problems Marines may

encounter while deployed. This instant access to knowledge fills gaps in training and allows Marines to continue to execute their mission in the absence of a technical expert. From solving complex Information Technology issues, to the correct employment of a heavy weapons system, deployed Marines can access virtually any information they need, or want, while deployed, without bringing bulky books. This ability does come at a cost, because more computers must be brought online to support these users. Now, the Lance Corporal looking up technical specifications of a 7 ton truck is generating traffic that is competing with the Commanding Officer's Video Teleconference (VTC). As the operators and maintainers become reliant on constant access to complete their jobs, work can come to a complete standstill if an outage occurs. The tactical Marine Corps is more efficient when they have access to online sources when deployed.

PowerPoint

Mission related emails are still an easy source of data reduction. The transfer of large Microsoft PowerPoint™ briefs, which is a common practice amongst garrison staffs, can be curtailed with a combination of technology and training.[39] Many times users just don't understand how a sending a large PowerPoint attachment can clog a network. If a user generates a 10 MB PowerPoint presentation and emails it to a distribution list that contains ten users at a node without an exchange server, that email has generated 100 MB of data. That large amount of data can virtually shut down a network for a significant time span, generating a backlog of traffic, compounding the problem. The Marine Corps reliance on PowerPoint to generate mission orders has driven more, sometimes unnecessary, graphics to be added to presentations, bloating a simple email into a network killer. If presentations must be made, users must be taught to use minimal, compressed, graphics, eliminate backgrounds, and use local storage device when

feasible to keep the network clear. A common practice on III MEF tactical networks is to automatically compress attachments with third party software. By educating users on the effect of large PowerPoint presentations and offering more efficient ways of transferring large files to other local users the number of large files transferred across the WAN can be reduced to a number that the satellite network can handle. The ultimate solution is to eliminate PowerPoint presentations altogether for a medium that is efficient in both communications and data storage. However, commercial practices, where presentations are flashy and bandwidth is virtually unlimited, do not support a trend to minimize file size.

VII. Recommendations:

To begin to provide stable reliable communications links across highly latent satellite networks the training and education of the Cyber Chief's, Cyber Defense Chief, Communications Chiefs, and Communications Officers must be improved, providing these Marines with the tools necessary to fully understand the traffic traversing their WAN links. The senior S/G-6 must have enough knowledge about mission essential programs and bandwidth requirements with the appropriate equipment and marines to complete the task. When bandwidth is at a premium the local cyber operators must have the ability to control traffic to ensure that mission essential traffic is not preempted by low or no priority traffic.

Data Reduction

Steps need to be taken by every unit in the chain of command to reduce their overall data requirements when operating off a tactical satellite network. Mainly users need to be educated about the impact that their traffic is having on the network. Communications officers must

develop and enforce tactics, techniques, and procedures that will substantially reduce traffic; these can be handled by local SOP. Some examples:

- PowerPoint presentations, when in field environments, should be kept to minimal graphics and color.
- Large files should be transferred via local shared drive instead of email.
- Default to mobile or low bandwidth, versions of websites.
- Proxy Servers should be implemented in the DDS-M to offer local copies of websites
- Third party compression software installed automatically.

Profiling POR/DOD Websites

Every program, application, or website that is controlled by the Department of Defense needs a network traffic profile conducted on it. From mission essential command and control programs to fitness report generation, every program that may be a requirement while on a satellite must have performance statistics provided to the S/G-6 that is providing the link. It is impossible for a local communications officer or chief make any educated guesses on the amount of bandwidth his unit will require when they have no knowledge of the data generated by required military applications. This task should fall to MCSC or MCOTEA to conduct live network analysis on programs while they are operated in tactical environments. An online network planning tool could be developed where a user can input their desired users and applications and an appropriate sided WAN link is suggested.

Commanders Intent

When a commander gets the news that, despite the amount requested, limited bandwidth is available for an exercise due to competing unit requirements, the commander must provide guidance to the unit on what will be allowed on the network. If only 2 Mbps is available, then decisions need to be make that may limit some staff sections ability to use their preferred programs. If the main focus of the mission rehearsal is to simulate kinetic operations, the commander may decide to eliminate all non secure web activity and go strictly with a secure network with CHAT being the primary means of communications. By eliminating non-secure web the bandwidth is reserved for C2 programs and mission essential traffic and it is unlikely the network will become congested. The commander may also offer NIPR hours, or a NIPR café as a means to limit the number of users to specific hours when its usage will be less likely to impact operations.

Proper Equipment and Manning to Perform Network Analysis

To properly manage Marine Corps networks at any level, from battalion up to base garrison networks, the proper equipment and training needs to be provided. Network security, in a civilian organization, would likely be run by a professional with a degree or extensive experience. Network management and shaping would be run by a different professional with similar credentials. The Marine Corps currently assigns these tasks to Cyber Defense Operators who are enlisted Marines that laterally moved into the MOS. The training of these Marines mainly focused on the defense and security of the network rather than traffic shaping, which leaves these Marines in short supply and overworked. To ensure that network traffic is properly controlled and shaped, skill needs to shift from Cyber Security to Cyber Operator,

communications officer, or chief. With simple tools like WireShark™ or SolarWinds™, the unit leadership would have the power to monitor high traffic clients and servers. Having this monitoring ability will at least give the leadership the capability to identify authorized, but excessive, users and get them to curtail their usage during mission essential times.

Quality of Service

The ideal solution to network congestion is a DoD wide network Quality of Service policy. QoS is a process where routers identify and prioritize traffic. However, for QoS to work properly all traffic must be properly identified and marked, especially at the source. QoS will allow VTC traffic to be properly prioritized and preempt web traffic. This will require traffic prioritization agreed upon by all DOD cyber organizations. Today, QoS on Marine Corps networks is rudimentary and does not account for the vast amount of programs and websites that are accessed. The QoS profile on the VSAT only identifies voice and classified traffic for prioritization and all remaining NIPRNet traffic is treated equally. For any solution to properly prioritize traffic, it will have to be implemented at the transport boundaries run by DISA. A DOD wide traffic shaping and prioritization profile must be created and implemented, which will require annual revisions and updates.[40]

Training

The Marine Corps doctrine is to train as we fight and the same must be true with cyber network. A unit conducting a forcible entry or a long range assault, similar to the march to Baghdad, will communicate mainly on classified networks with a chat program.[41] The only programs the commander will be concerned with will be those that show them their common operational picture (COP) and allow them to transfer basic information between themselves and

their adjacent units. Units need to train in environments where they choose only the most important network requirements and prohibit all other traffic. Morning Reports, Fitness Reports, MarineNet classes should be left in garrison and force Marines to plan ahead because those sites will be unavailable on the satellite in a communications restricted environment.[42] The return to the basics must include radio as a primary means of communication. The resurgence of HF radios, combined with new equipment being fielded, will allow a unit to remain connected in satellite denied environment. The future wideband High Frequency radios will provide a sufficient data rates to allow chat and small data imagery to be transferred hundreds of miles without a satellite link. Training plans should provide a wide range of simulated tactical environment. Training should range from radio only to full scale Combat Operations Center (COC) operations. The different scenarios will ensure data planners and operators fully understand the cyber needs of the unit.[43]

VIII. Summary

The Marine Corps must re-learn how to operate with a minimum network footprint as possible to complete missions. Units deployed to Desert Storm and Operation Iraqi Freedom completed complex missions with bandwidth that would be considered unacceptable in today's Marine Corps. As users' digital presence in garrison and at home has increased so has the call for more tactical bandwidth. More bandwidth is currently not available and will definitely not be available in future conflicts. The communications officers and chiefs must stop asking for more bandwidth and begin to train network operators and users on proper network management. In the initial stages of a conflict commanders should expect to have low bandwidth means of communication, such as telephone or text based chat services. Video Teleconference and large PowerPoint's have become standard practice for MEF and Division level commanders to

communicate orders and these are unlikely to be available during future conflicts. Learning to operate in austere conditions, as espoused by the Marine Operating Concept, does not mean bringing more garrison networks to the field.[44] Commanders play the key role in this management and they will have to make difficult decisions on what are mission essential programs and which must be prohibited to ensure network traffic does not congest the WAN.

The Marine Corps leverages new technology to fight and win the nation's wars. It should not stay stuck in the past world of paper orders and single channel radio. However, there may come a time when that is all that is available and Marines must train to that standard. The war is not won by the most modern logistic system or a flashy PowerPoint, it is won by the men and women whose intelligence and experience drives the mission. As a middleweight, expeditionary force, the Marine Corps must move and communicate quickly and an overreliance on big data is a hindrance. Just as Marines strive for gear accountability, they must strive to be efficient with every bit of data. To do more with less is a motto that served the Marine Corps well when it came to equipment and it should be applied to our network needs as well.

---

[1] Kenneth Y. Jo. *Satellite Communications Network Design and Analysis*. (Norwood, US: Artech House Publishers,2011), 121.
[2] Ibid, 124
[3] Hiranya Jayathilaka, Harshana Porawagama, Muditha Thelisinghe, and Kaushalya Amarasinghe. *Network Resource Utilization and Social Networking*. (Sri Lanka: University of Moratuwa, 2009), 4.
[4] Thomas P. Cavaini, "Tools and Techniques for Simplifying the Analysis of Captured Packet Data." *Journal of Information Systems Education, Vol. 19(4),* (2008): 378.
[5] Department of the Navy, United States Marine Corps. *The Marine Operating Concept.* (Quantico VA: Headquarters Marine Corps, 2016), 6.1.1.
[6] Department of the Navy, United States Marine Corps. *MAGTF Communications Systems.* Warfighting Publication (Washington DC : Headquarters Marine Corps, 2010), 5-8.
[7] Office of the Joint Chiefs of Staff. *Joint Publication 6-0, Joint Communications System.* Joint Publication, (Washington D.C. : Department of Defense, 2015), II-2.
[8] DoD Chief Information Officer. *Unified Capabilities Master Plan.* (Washington D.C.: Department of Defense, 2011), 3.

[9] Neller, Robert B. *FRAGO 01/2016: Advance to Contact.* (Quantico VA: United States Marine Corps, 2016), 8.
[10] Paulo Alves, Major USMC (Cyber Network Operations Officer), Discussion with author, Jan 17, 2017.
[11] Department of the Navy, United States Marine Corps. *MAGTF Communications Systems.* Warfighting Publication (Washington DC : Headquarters Marine Corps, 2010), 2-5.
[12] Ibid 3-4.
[13] Information Sciences Institute. *Transmission Control Protocol, DARPA Internet Program, Protocol Specification. Request for Comment (RFC 793),* (Marina Del Rey, California: Defense Advanced Research Projects Agency, 1981), 1.
[14] Richard W. Stevens, *TCP/IP illustrated (vol. 3): TCP for transactions, HTTP, NNTP, and the Unix domain protocols* . (Redwood City, CA: Addison Wesley Longman Publishing Co., Inc., 1996), 689.
[15] Information Sciences Institute. *Transmission Control Protocol, DARPA Internet Program, Protocol Specification. Request for Comment (RFC 793),* (Marina Del Rey, California: Defense Advanced Research Projects Agency, 1981), 5.
[16] Paulo Alves, Major USMC (Cyber Network Operations Officer), Discussion with author, Jan 17, 2017.
[17] Comtech EF Data. "Comtech EF Data TurboIP-G2 Performance Enhancement Proxy." http://www.satcomresources.com. March 2017. http://www.satcomresources.com/Comtech-EF-Data-turboIP-G2-Performance-Enhancement-Proxy (accessed March 19, 2017).
[18] Gartner,Inc. *Magic Quadrant for WAN Optimization.* July 21, 2016. https://www.gartner.com/doc/reprints?id=1-36UZLWA&ct=160517&st=sb (accessed March 19, 2017), 3.
[19] Headquarters Marine Corps. *GCSS-MC Increment 1 Version 0.6, Network Communications Guidebook.* Marine Corps Publication, (Washington, DC: Headquarters Marine Corps, 2015), 7.
[20] Ibid, 9.
[21] Ibid, 11.
[22] Alexander Ochoa, "Supply C2 Support." *Marine Corps Gazette 100*, 2016: 76.
[23] Paulo Alves, Major USMC (Cyber Network Operations Officer), Discussion with author, Jan 17, 2017.
[24] Department of the Navy, United States Marine Corps. *MAGTF Communications Systems.* Warfighting Publication (Washington DC : Headquarters Marine Corps, 2010), 5-9.
[25] Paulo Alves, Major USMC (Cyber Network Operations Officer), Discussion with author, Jan 17, 2017.
[26] Office of the Joint Chiefs of Staff. *Joint Publication 6-0, Joint Communications System.* Joint Publication, (Washington D.C. : Department of Defense, 2015), A-2.
[27] Paulo Alves, Major USMC (Cyber Network Operations Officer), Discussion with author, Jan 17, 2017.
[28] Ibid
[29] Ibid
[30] U.S. Marine Corps Concepts and Programs. *Tactical Networking Systems (TNS).* June 1, 2015. https://marinecorpsconceptsandprograms.com/programs/command-and-controlsituational-awareness-c2sa/tactical-networking-systems-tns (accessed March 20, 2017), 1.
[31] Paulo Alves, Major USMC (Cyber Network Operations Officer), Discussion with author, Jan 17, 2017.

[32] Thomas P. Cavaini, "Tools and Techniques for Simplifying the Analysis of Captured Packet Data." *Journal of Information Systems Education, Vol. 19(4)*, 2008, 380.
[33] Paulo Alves, Major USMC (Cyber Network Operations Officer), Discussion with author, Jan 17, 2017.
[34] Craig S. Clark, "Open Source Intellgence: An Oxymoron or Real Intelligence?" *Marine Corps Gazette*, 2015: 22.
[35] Hiranya Jayathilaka, Harshana Porawagama, Muditha Thelisinghe, and Kaushalya Amarasinghe. *Network Resource Utilization and Social Networking*. (Sri Lanka: University of Moratuwa, 2009), 5.
[36] Richard W. Stevens, *TCP/IP illustrated (vol. 3): TCP for transactions, HTTP, NNTP, and the Unix domain protocols* . (Redwood City, CA: Addison Wesley Longman Publishing Co., Inc., 1996), 688.
[37] Susan W. Durham, "In their Own Words: Staying Connected in a Combat Environment." *Military Medicine 175*, 2010, 556.
[38] Brian McCombs, "Preparing for and Providing Intermediate Supply Support." *Marine Corps Gazette 98*, 2014: 35.
[39] Paulo Alves, Major USMC (Cyber Network Operations Officer), Discussion with author, Jan 17, 2017.
[40] DoD Chief Information Officer. *Unified Capabilities Master Plan.* (Washington D.C.: Department of Defense, 2011), 4.
[41] Paulo Alves, Major USMC (Cyber Network Operations Officer), Discussion with author, Jan 17, 2017.
[42] Atiim Phillips, *Position Paper on Training in a C4 Degraded or Ddenied Environment* . Position Paper, (Okinawa, Japan: 3d MEB, II MEF, 2017), 6.
[43] Ibid 9.
[44] Department of the Navy, United States Marine Corps. *The Marine Operating Concept.* (Quantico VA: Headquarters Marine Corps, 2016), 6.1.1.

Bibliography

Cavaini, Thomas P. "Tools and Techniques for Simplifying the Analysis of Captured Packet Data." *Journal of Information Systems Education, Vol. 19(4)*, 2008: 375-378.

Clark, Craig S. "Open Source Intellgence: An Oxymoron or Real Intelligence?" *Marine Corps Gazette*, 2015: 22-25.

Comtech EF Data. "Comtech EF Data TurboIP-G2 Performance Enhancement Proxy." *http://www.satcomresources.com.* March 2017. http://www.satcomresources.com/Comtech-EF-Data-turboIP-G2-Performance-Enhancement-Proxy (accessed March 19, 2017).

Department of the Navy, United States Marine Corps. *MAGTF Communications Systems.* Warfighting Publication, Washington D.C. : Headquarters Marine Corps, 2010.

Department of the Navy, United States Marine Corps. *The Marine Operating Concept.* Quantico VA: Headquarters Marine Corps, 2016.

DoD Chief Information Officer. *Unified Capabilities Master Plan.* Washington D.C.: Department of Defense, 2011.

Durham, Susan W. "In their Own Words: Staying Connected in a Combat Environment." *Military Medicine 175*, 2010: 554-559.

Gartner,Inc. *Magic Quadrant for WAN Optimization.* July 21, 2016. https://www.gartner.com/doc/reprints?id=1-36UZLWA&ct=160517&st=sb (accessed March 19, 2017).

Headquarters Marine Corps. *GCSS-MC Increment 1 Version 0.6, Network Communications Guidebook.* Marine Corps Publication, Washington, DC: Headquarters Marine Corps, 2015.

Information Sciences Institute. *Transmission Control Protocol, DARPA Internet Program, Protocol Specification.* Request for Comment (RFC 793), Marina Del Rey, California: Defense Advanced Research Projects Agency, 1981.

Jayathilaka, Hiranya, Harshana Porawagama, Muditha Thelisinghe, and Kaushalya Amarasinghe. *Network Resource Utilization and Social Networking.* Sri Lanka: University of Moratuwa, 2009.

Jo, Kenneth Y. *Satellite Communications Network Design and Analysis* . Norwood, US: Artech House Publishers, 2011.

Kemp, Jesse, and Daniel Bartos. "Can we "Fight Tonight" with GCSS-MC?" *Marine Corps Gazette 97*, 2013: 26-29.

McCombs, Brian. "Preparing for and Providing Intermediate Supply Support." *Marine Corps Gazette 98*, 2014: 34-36.

Neller, Robert B. *FRAGO 01/2016: Advance to Contact.* Quantico VA: United States Marine Corps, 2016.

Ochoa, Alexander. "Supply C2 Support." *Marine Corps Gazette 100*, 2016: 76-77.

Office of the Joint Chiefs of Staff. *Joint Publication 6-0, Joint Communications System.* Joint Publication, Washington D.C. : Department of Defense, 2015.

Phillips, Atiim. *Position paper on training in a c4 degraded or denied environment* . Position Paper, Okinawa, Japan: 3d MEB, II MEF, 2017.

Stevens, W. Richard. *TCP/IP illustrated (vol. 3): TCP for transactions, HTTP, NNTP, and the Unix domain protocols* . Redwood City, CA: Addison Wesley Longman Publishing Co., Inc., 1996.

U.S. Marine Corps Concepts and Programs. *Tactical Networking Systems (TNS).* June 1, 2015. https://marinecorpsconceptsandprograms.com/programs/command-and-controlsituational-awareness-c2sa/tactical-networking-systems-tns (accessed March 20, 2017).

THIS PAGE INTENTIONALLY LEFT BLANK

Appendix A: Commonly Requested Programs

DCIPS	Defense Civilian Intelligence Personnel System
3270.00	Force Management Software
Acrobat Distiller	Commercial Software
Adobe Connect	Commercial Software
Adobe Connect	Commercial Software
Adobe Pro	Commercial Software
AEMIT-EWRB	Asset Enterprise Management Information Tool - Electronic Weapons Record Book
AFATDS <A>	Advanced Field Artillery Tactical Data System
AHLTA	Armed Forces Health Longitudinal Technology Application
AMHS	automated message handling system
APAN	All Partners Access Network
APES	Automated Performance Evaluation System
ARCCatalog	Geoprocessing Tool
ARCMap	Geoprocessing Tool
BAT-HIIDE	Biometric Automated Toolset - Handheld Interagency Identity Detection Equipment
BCS3	Battle Command Sustainment Support System
BENEFEDS	Benefits Federal Employees
BUPERS	Bureau of Naval Personnel
C2PC <C>	Command and Control Personal Computer
CIHEP	Counterintelligence and Human Intelligence Equipment Program
CitiDirect	CitiBank Direct
CLC2S	Common Logistics Command and Control System
CPIMS	Continuous Process Improvement Management System
CPOF <C>	Command Post of the Future
DASH	Discrimination and Sexual Harassment
DCGS-MC EDS	Distributed Common Ground-Surface System Marine Corps / Enterprise DIB Services
DCPDS	Defense Civilian Personnel Data System
DCPS	Defense Civilian Pay System
DDSM	Data Distribution System-Modular
DEERS	Defense Enrollment Eligibility Reporting System
DenCas	Dental Common Access System
DEOCS	Defense Equal Opportunity Command Survey
DFAS/MY PAY	Defense Finance and Accounting Services
DMM	Drill Management Module
DRRS-MC	Defense Readiness Reporting System-Marine Corps

DSAIDS	Defense Sexual Assault Incident Database
DTMS	Digital Training Management System
DTS	Defense Travel System
EBIS	Employee Benefits Information System
ENVI	Environment for Visualizing Images
ESXi	Elastic Sky X Integrated
FBCB2 BFT	Force XXI Battle Command Brigade and Below-Blue Force Tracker
FltTemps	Fleet Training Management Planning System
Fortinet	Commercial Firewall Software
GBOSS	Ground-Based Operational Surveillance System
GCSS-MC	Global Combat Support System-Marine Corps
Google Earth	Commercial Mapping Software
HBSS	Host Based Security System
IAPS	Improved Awards Processing System
IAS FOS <B>	Intelligence Analysis System Family of Systems.
ICODES	Integrated Computerized Deployment System
IDMS	Integrated Database Management System
IGC	Integrated Development Environment/Global Transportation Network Convergence
Intel Svr Windows	Intelligence Operating System Server
IntelShare SharePt	Collaboration Software
IOS v1	Intelligence Operating System Version 1
iRAPT	Invoicing, Receipt, Acceptance, and Property Transfer
IRC XPro	Internet Relay Chat X Professional
JADOCS	Joint Automated Deep Operations Coordination System
JBV	Joint Battlespace Viewer
JEM	Joint Tactical Radio System (JTRS) Enhanced Multiband Inter/Intra Team Radio (MBITR)
JFRG II	Joint Force Requirements Generator II
JWARN	Joint Warning and Reporting Network
MAKO	Chat Program
MARINE NET	Marine Network
MCAT	Marine Command Aircrew Trainers
MCATS/DON Tracker	Marine Corps Action Tracking System/ Department of Navy Tracker
MCMEDS	Marine Corps Medical Entitlements Data Systems
MCMPS	Marine Corps Mobilization Processing System
MCTFS	Marine Corps Total Force System
MDSS II	MAGTF Deployment Support System II
MERIT <D>	Marine Corps Equipment Readiness Information Tool
MOL	Marine On Line

MROWS	Marine Reserve Order Writing System
MRRS	Medical Readiness Reporting System
MS Exchng 2010	Microsoft Exchange
NavFit98B	Navy Fitness Report
NAVMED & PERS	Navy Medicine and Personnel
NetApps	Network Appliance Incorporated
NFAAS	Navy Family Accountability and Assessment System
NISPS	Navy Standard Integrated Personnel System
NKO	Navy Knowledge Online
OpenFire	Collaboration Software
Palantir	Commercial Software
PFPS	Portable Flight Planning Software
PR Builder	Procurement Requirement Builder
PSS-SOF	Precision Strike Suite - Special Operations Force
Remedy	Commercial Help Desk Software
RF ITV	Radio Frequency In-Transit Visibility
SABRS	Standard Accounting Budgeting and Reporting System
SharePoint	Commercial Collaborative Software
SLDCADA	Standard Labor Data Collection and Distribution Application
SMARTS	SABRS Management Analysis Retrieval System
SMS	Single Mobility System
Socet GXP	Softcopy Exploitation Tool Geospatial eXploitation Products
Solar Winds	Network Monitoring Software
StrikeLink	Aviation Program of Record
TAMIS	Total Ammunition Management Information System
TBMCS	Theater Battle Management Core System
TCPT	Transportation Capacity Planning Tool
TEG FOS	Tactical Exploitation Group Family of Systems
TFSMS	Total Force Structure Management System
TFSMS	Total Force Structure Management System
TLCM-OST	Total Life Cycle Management Operational Support Tool
TPC FOS	Topographic Production Capability Family of Systems
Transverse	Commercial Chat Program
TWMS	Total Workforce Management System
VMware Server	Virtual Machine softWare Server
Vsphere	Virtual Machine Client Software
WAWF	Wide Area Work Flow
WEBO	Web Orders

WESS	Web Enabled Safety System
Win 08/12 Server	Windows Server Operating System
WSUS	Windows Service Update Server