Unit computer pitfalls

Part I

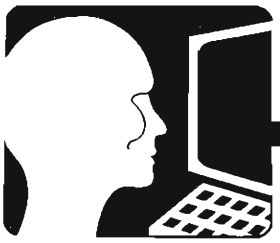
by Capt. Peter M. Murphy

This August, some will celebrate the 12th anniversary of the first microprocessor. It seems incredible that just over a decade ago the pocket calculator was a faint dream and that the personal computer was something seen only in science fiction. Today it does not require a crystal ball to predict that by the turn of the century for every home with a television there will be a personal computer. Not long ago a college freshman was required to own a slide rule to study engineering. By 1975, all freshmen studying any of the sciences were required to own an electronic calculator. Today, several universities require all freshmen to purchase a personal computer.

In light of this trend, and combined with the goal of automating the battlefield, it is no surprise that the personal computer has found its way into the Army in great numbers. There are many units which have used large numbers of microcomputers to automate administrative functions and to improve their readiness training. The XVIII Airborne Corps will be using a large number of Apple computers to facilitate information distribution among its tactical operations centers. At Fort Stewart, GA, the 24th Infantry Division is testing the use of TRS-80 computers in improving the Army Logistics System under project SMART. In March of this year the Tactical Management Information Systems (TACMIS) of the Computer Systems Command requested proposals for development of the Tactical Army Combat Service Support Computer System (TACCS). This will be a transportable, user-friendly, commercially available, off-the-shelf, computer and software system to be used on the battlefield for combat service support missions at varied levels of command. TACMIS is anticipating the purchase of 2500 to 6000 systems.

Yet in spite of the benefits of this rapidly expanding technology and its growing availability, I must fly the flag of caution. This article will examine many of the truths that are seldom revealed to the potential owner of a personal computer.

The first problem to face the proud new owner of a microcomputer is the hardware—the actual electronics themselves. It does not take long to discover that every computer is different and that selecting the right one can be more bewildering than buying your first automobile. This article will not address how to decide upon the right computer as that will be the topic of Part 2. The reason for the seemingly infinite variations from one microcomputer to another is the almost total lack of standards within the microcomputer industry. This lack of standardized hardware presents a greater problem than just confusing the issue of choosing the best microcomputer. For once a particular computer is procured, it will dictate all future choices of both additional hardware and software (the computer programs). The microcomputer industry has not yet evolved to the stage of modular interchangability that we take for granted when putting together a stereo system where any speaker may be used with any amplifier. With some brands of microcomputers, the owner must purchase additional peripherals (such as printers, tape and disk memory units) from the same manufacturer. For example, a disk drive made for a Radio Shack computer will not operate with an Apple computer and vice versa. When it becomes desirable to upgrade a present microcomputer system with new hardware, the unwary owner may find that many, if not all, of the peripheral equipment will have to be replaced.



A second obstacle created by the lack of standardization of computer hardware is that it inhibits software portability; that is, it hinders the ability to take a program from one computer and run it on another type of computer. Each computer has its own unique machine language that is determined by the microprocessor that is found inside the computer. The IBM Personal Computer (PC), for example, uses an Intel 8088 while the Osborne I uses a Zilog Z80A; thus, a program written specifically for the IBM PC cannot be used on the Osborne. Theoretically, a program written in a high-level language such as BASIC will be machine independent and thus transportable. However, not all computers are capable of using the same high-level languages. Most (though not all) personal computers offer some form of BASIC and some have the option of being programmed in languages such as COBOL, FORTRAN, Pascal, C and others. It can be extremely frustrating if the program you need is written in a language that is not available on the computer you own. Using a common high-level language may seem like a logical solution, yet here again the various manufactures have placed another barrier. In order to make their respective computers more attractive, most companies offer their own versions of BASIC as well as other high-level languages. There is enough difference between the BASIC offered on the Texas Instruments TI-99/4A computer and the BASIC offered on the VIC 20 so that the same program will not run on both computers without significant changes. Even when two computers use the very same microprocessor, the problem of software portability is still not solved. Both the Apple II and the Atari 800 use the MOS 6502 microprocessor, yet they cannot share programs because they each have a unique operating system. The operating system is the manufacture supplied program that is always in the computer and determines what commands the computer will understand and how the computer will interface with its peripheral devices. So even if two computers are identical in every way except their operating system, they may not be able to share their programs because the operating systems may record the program on the magnetic disk using different formats. This renders the disk unreadable by any other computer. Though there are many fine programs that are available free within the Army for helping with such applications as personnel activities, supply/accountability, frequency analysis, and communications planning; these programs cannot be shared because the Army has not controlled the purchase of microcomputers by individual units to ensure interoperability.

A third problem created by nonstandard hardware is just now becoming evident. As more and more units automate various functions, it will become increasingly difficult to train personnel because each unit will perform these tasks a little differently and the equipment will vary from unit to unit. Thus, instead of a clerk learning a standard way of recording supply transactions only once, they may have to learn a new way every time they PCS.

Aside from the variations in microcomputer hardware, the users must be aware of all special environmental requirements that may exist. Though all microcomputers are solid state electronic devices, not all of them are rugged enough to survive the stress of tactical operations. Frequently, dust, heat, and humidity can be hazardous to many of the delicate components of an off-the-shelf personal computer. The memory within the computer is volatile, which means that the slightest loss of power may result in the total loss of eveything in memory. This problem became very frustrating for a signal battalion at Fort Gordon, GA, which has a word processor located in its PAC. Until special precautions were taken, the contents of its memory were scrambled every time the photocopy machine was turned on because they shared the same power circuit. This problem would be greatly magnified in a tactical environment where small generators supply power. Also, the medium for permanent storage of information such as magnetic tape and magnetic disks is highly susceptable to the radiation produced by a common TV, generator, electric typewriter, or other electrical appliance. Placing a tape or disk too close to one of these devices could result in a partial loss of information. Finally, if there is a requirement for communications betwen computer systems a thorough evaluation must be made. Frequently, existing telephone lines on Army installations lack the quality to provide reliable and error free service for data communications.

Once a computer is procured, it is still useless to the unit until there is some functional software available to bring the electronic beast to life. Recently, an office at Fort Gordon acquired a rather sophisticated microcomputer to maintain records. The assistance of the author was sought to explain how these records could be developed using the built-in filing program on the computer. It had to be explained that the program in question could in no way perform the desired task and that the computer, without any additional software, was without value to that office. This was a very expensive lesson learned. Everyone contemplating using a personnel computer to automate some job in the Army must realize that there is presently no agency of any kind developing software for these machines. So where does the military computer owner go to obtain software? First, you may try using or adapting commercially available software. This software is usually well written and easy to use though it may sometimes cost as much as the computer itself. Another problem with commercial software is that it is seldom tailored for military application and may require extensive modification before it is appropriate for military use.

A second source of software is that written by the individual using the computer. This certainly has the advantage of being assured of getting exactly what you want. However, the more specific a piece of software is, the less likely it becomes that that software can be utilized by another unit. There are more serious problems created by using software written by a novice than just its inflexibility. Most "home brewed" programs are poorly written and unprofessional. Combine this with the fact that most also lack sufficient documentation and it becomes a near impossibility to modify these programs later on. Any program used over a long period of time will eventually require

modifications and updating as changes to Army Regulations and doctrine alter the way the jobs that have been automated are done. Additionally, it may become desirable to expand the capabilities of the software. If all of this is made difficult by the fact that the software was written by a novice who has long since left the unit, then the only alternative is to start from scratch. In fact, this happened in one company in which the commander had written his own personnel management programs on his Apple II. The change-of-command included the purchase of the computer and programs by the incoming commander who later found the programs to be inadequate. After many attempts to modify the existing programs he realized that starting anew would be far easier. Another trap frequently encountered by novice programmers is that they may be the only individuals who can operate the program. When a program requires an intimate knowledge of its workings to use it, we say that the software is not "user friendly." This software is usually of little value after the author leaves the unit. Finally, whenever individuals write their own software there is no quality control to ensure that the procedures comply with regulations and doctrine. Units must be cautious of changing standard operating procedures just because it will make it easier to automate the job.

So where does a unit turn to obtain quality software? Each major command must have available an Automation Management Office (AMO) to interact with and coordinate processing activities. The AMO should be aware of other units within the command that have acquired microcomputers and what they are being used for. Additionally, DA Pamphlet 18-1-1, Army Inventory of Data Systems (AIDS), is a microfiche catalog of data systems currently in use or under development. This catalog is updated and distributed quarterly. Unfortunately, there may be very little information that is appropriate for microcomputers. There is, however, an organization specifically devoted to assisting the user of microcomputer systems in the Army. It is the Command and Control Microcomputer Users' Group (C2 MUG). The address to correspond with the users' group and to receive the monthly publication, C2 MUG BULLETIN, is: Chief, CECOM, SDSC, ATTN: DRCPM-OTDS-SDSC (C2 MUG), Ft. Leavenworth, KS 66027. The C2 MUG may also be reached by telephone (913) 684-7500, or AUTOVON 552-7500. Another source of information on military applications of microcomputers is the Navy Regional Data Automation Center. This organization publishes a monthly newsletter on small computers titled CHIPS AHOY. Communications should be addressed to: CHIPS AHOY, Navy Regional Data Automation Center, Norfolk, VA 23511 or telephone: (804) 444-8486.

The Army guidelines for security of all computer systems (which includes all microcomputers) are contained in AR 380-380, Automated Systems Security. This regulation is applicable to "intelligent terminals, minicomputers, microprocessors, and some word processing systems. This regulation describes the following basic DOD computer system policies.

Individual accountability. Each user's identity will be positively established, and their access to, and activity in the system (including material accessed and actions taken) controlled and open to scrutiny. This implies that some sort of account numbers and passwords are required for each user of the system.

Environmental control. The computer system will be externally protected to minimize the likelihood of unauthorized access to system entry points, access to classified information in the system, or damage to the system.

System stability. All elements or components of the computer system will function in a cohesive, identifiable, predictable, and reliable manner so that malfunctions are detected and reported within a known time.

Data integrity. Each file or collection of data in the computer system will have an identifiable origin and use. Its accessibility, maintenance, movement, and disposition shall be governed on the basis of security classification and need-to-know.

System reliability. The system should function so that all users have access to all of the information to which they are entitled, but no more.

Communication links. These links and lines will be secured in a manner appropriate for the material designated for transmission through such lines or links. For further guidance and policy concerning the transmission of official information see AR 380-51.

Classified and sensitive unclassified material. Such material handled and produced by the computer system or stored in or on media will be safeguarded as appropriate for the classification or sensitivity assigned. It should be noted that information does not have to be classified to be considered sensitive and thus subject to special considerations. Any computer that processes asset/resource accounting or authorization data greater than $10,000,000 (such as an automated property book) is considered Critically Sensitive and on the same level as CONFIDENTIAL information. A system that processes information requiring protection under the provisions of the Privacy Act of 1974 (such as unit personnel records) is considered Highly Sensitive. All computer systems that process classified or sensitive material must be properly accredited. Accreditation procedures are explained in detail in AR 380-380. One fact that is not obvious to the normal computer user is that just because a classified file is deleted from a computer disk, that disk is not declassified. It is a relatively simple task for a knowledgable individual to retrieve that information from the disk even though it appears to have been removed. The proper methods of declassifying computer storage media are described in AR 380-380.

If a data processing activity maintains classified defense information, then steps must be taken to control compromising emanations (TEMPEST) as established in AR 530-4. Most electronic devices including printers, disk and tape drives, and especially cathode ray tube (CRT) type displays are sources of compromising emanations which could be intercepted by unauthorized individuals. There are three basic methods recommended for controlling TEMPEST. First, to provide the equipment with a physical control zone (PCZ) of sufficient spherical diameter to preclude successful hos-

tile intercept action. Second, to implement minimum essential countermeasures to contain compromising signals within the accepted PCZ. Third, to design or modify the equipment to limit the strength of compromising signals to acceptable limits. Some microcomputers manufactured today are being designed to satisfy TEMPEST criteria. The Grid Compass by Grid Systems of Mountain View, CA, is one such system that hopefully will meet all military and TEMPEST specifications. Since it is highly transportable (weighing only nine pounds and measuring 15 by 11 1/2 by 2 inches) it is of particular interest to the Army.

The final problem that a unit should be concerned about is dependency on the computer that may develop. There have been many instances where a member of a unit will use their personally owned computer in their job on their own initiative. While this may improve the operations of a unit in garrison, it will be a disastrous lesson for that unit when it mobilizes and the computer cannot go to the field with it. Too often the presence of a computer causes manual record keeping to be neglected and doctrinal skills to deteriorate from disuse. Eventually it comes time for the individual who owns the computer to transfer. The commander may then have to purchase the computer and its software because the unit cannot operate without it. This also leaves the door open to a much more common situation: when the hardware simply fails. You cannot hold a floppy diskette up to the light and read the information recorded on it; you have to have the machine to retrieve the data. And again, unit personnel become so accustomed to using the computer that they forget how to do things manually.

For everyone who has not discovered the joy of computing, there are these final bits of wisdom. The first rule of automation: always make a backup copy! This lesson has been learned the hard way by most everyone that has worked with a computer. The Property Book Officer of a signal battalion on Fort Gordon recorded the property book on the battalion's word processor in a convenient file. Many hours were wasted when the only copy of that file was accidentally erased. The second rule of automation: don't use your backup copy until you make another copy!

This article has examined some of the common problems encountered in the world of automation. Its purpose is certainly NOT to discourage automation or the use of personal computers. However, an informed decision is a better decision. Once the decision has been made to obtain a personal computer then the difficult process begins of choosing the right one.

I would like to thank the members of the Communications-Electronics Technology Branch of the Officer Advanced Division, Officers Department for their technical and writing assistance.

Capt. Murphy holds an ROTC commission from Iowa State University where he also earned a BS in electrical engineering and another in computer engineering. Before entering the military, Murphy was involved with computer security experiments at NSA.

AC will publish Part II of Murphy's article in the fall issue. In it, he discusses which computer is right for your office.