COMPUTER VIRUSES IN ELECTRONIC WARFARE

By Dr. Myron L. Cramer and Stephen R. Pratt

The application of computer virus concepts has made possible the advent of a new class of electronic warfare.

Events of the last few years have demonstrated dramatically that computer viruses are not only feasible but can quickly cause catastrophic disruption of computer systems and networks.

Current trends in the development of military electronic systems have significantly increased the vulnerability of these systems to computer virus attack. This has created a new form of electronic warfare consisting in the electronic insertion of computer virus microcode into a victim electronic system through direct or indirect mechanisms.

This paper discusses the application of computer virus techniques to electronic warfare from both an offensive and a defensive perspective.

Background

Defense Electronics

Military electronic systems have historically included a wide variety of sensors, control systems, communications, and electronic warfare equipments. *Sensors* include radars, infrared systems, electro-optical systems, and lasers and fill many critical functions including monitoring system operation and target development. *Control* systems include navigation, autopilot systems, guidance systems, and stabilizer systems. *Communications* systems provide connectivity among participants for the distribution of mission tasking and the exchange of data. The trend over the last two decades has been for defense weapon systems to make increasing use of electronics, especially in the form of built-in, or *embedded* computers. As implementing technology has become available, it has become more efficient to implement system functions through software programmed for these embedded computers. Additionally, increased automation of weapon systems has led to greater uses of computerized digital communications.

Electronic Warfare

As sensor systems such as radar came into usage during World War II, electronic countermeasures were developed to deny an adversary the benefits of this technology. The field of Electronic Warfare has evolved to develop techniques, technologies, and systems to deny an adversary the use of the electromagnetic spectrum and to protect our uses. *Electronic warfare* systems provide threat warning, platform self-protection, and countermeasures against threat systems using the electromagnetic spectrum.

Computer Viruses

Computer viruses once existed only in theory. The computer virus concept refers to computer code that, in a manner analogous with biological viruses (1) can *infect* another program, and (2) and acting through an infected program can *reproduce* itself and spread within a host computer system. In the last few years, several widely publicized computer viruses have drawn increased attention to these virus programs. No longer an oddity, virus programs repeatedly show up in many large computer operations, despite attempts to isolate and eradicate these disruptive intruders.

The demonstrated characteristics of computer viruses include several remarkable items, including size, versatility, propagation, effectiveness, functionality, and persistence.

Size. The sizes of the program code required for computer viruses has been demonstrated to be surprisingly small. This has facilitated the ability of these programs to attach themselves to other applications and escape notice for long periods of time.

Versatility. Computer viruses have appeared with the ability to generically attack a wide variety of applications. Many do not even require information about the program they are infecting.

Propagation. Once a computer virus has infected a program, while this program is running, the virus is able to spread to other programs and files accessible to the computer system. The ability to propagate is essential to a virus program.

Effectiveness. Many of the computer viruses that have received widespread publicity have had far-reaching and catastrophic effects on their victims. These have included total loss of data, programs, and even the operating systems.

Functionality. A wide variety of functions has been demonstrated in virus programs. Some virus programs merely spread themselves to applications without otherwise attacking data files, program functions, or operating systems activities. Other virus programs are programmed to damage or delete files and systems. The effectiveness of these programs is enhanced through the use of several phases of operation, in which the virus propagates through a system or lies dormant until triggered by a specified event. This allows the virus program increased time to spread before the victim system's user becomes aware of its presence.

Persistence. Even after the virus program has been detected, recovery of data, programs, and even system operation has been difficult and time consuming. In many cases, especially in networked operations, eradication of viruses has been complicated by the ability of the virus program to repeatedly spread and reoccur through the networked system from a single infected copy.

Relationship of Computer Viruses to Traditional ECM

Table 1 compares the relationship between computer viruses and traditional forms of electronic countermeasures (ECM). As shown in this table (and with few exceptions), electronic countermeasure systems have functioned by targeting the *receiver* elements in electronic systems. By contrast, computer viruses have the potential to operate by targeting the victim system's *processors,* and can be used to target a wider set of electronic systems.

Table 1. Comparison between Computer Viruses and Traditional ECM

	TRADITIONAL ECM	COMPUTER VIRUSES
Target Systems	Sensors Control Systems Communications	Computerized and networked electronic systems
Targeted Elements	Receivers	Processors
Jamming Techniques	Noise Deception	Deception Manipulation
Jamming Implementation	Primarily analog	Digital

Early countermeasure systems operated by simply increasing the noise level at the victim receiver, thus disrupting its ability to receive its intended signal. As designs of communications and radar equipments were refined through the use of improved coding and signal processing techniques, they became capable of reliable operation with lower signal to noise ratios. EW systems achieved greater jamming efficiency by optimizing noise frequency distribution through the use of comb and other jamming patterns.

As communications and radar systems utilize highly sophisticated signal processing, noise jamming systems (especially airborne self-protection radar jammers) become less effective if they work at all. Deception jamming exploits specific characteristics of targeted system's receiver and RF processing. Deception jamming is covert and operates with the system operator unaware that he is being countered. One example includes the use of *squelch-tone capture* techniques against tactical radios. In this technique, a jammer transmits a jamming tone that simulates one used by the radio being jammed. The victim receiver accepts this squelch tone and increases its squelch setting, thus cutting-off the transmitted signal it should be receiving. The intended receiver hears nothing, and is unaware of either its communications or the jamming. Another example is the use of *range-gate pull-off* techniques against tracking radars. In this technique, an EW system aboard an aircraft first amplifies and repeats the tracking pulses. Successive transmissions are systematically delayed by increasing amounts with the result that the tracking radar's range gate is drawn away from the target.

Computer viruses offer similar capabilities to deception jamming in that they operate covertly, at least initially while they propagate through a system. However, since computer viruses exploit the victim system's processor, the manner in which they achieve their effects is different. Additionally, they can be used to target a wider set of weapon system functions.

Modern communications and radar anti-jam technology has created the need for new countermeasures techniques and technologies. While there have been many successful countermeasure systems, there are several areas that have resisted the development of reliable countermeasure solutions, for example, self-protection for large aircraft, techniques against netted monopulse radars, land-line communications, and packet-switched communications networks. In devising systems to counter newer netted digital systems, computer viruses can provide the designer an additional category of jamming capabilities from which to select options. Once these capabilities are fielded, they can provide the tactical commander with an unparalleled set of capabilities.

Characteristics of Computer Viruses in EW

Making use of the unique features of computer viruses, Computer Virus EW have several unique characteristics which affect their applicability to tactical operations.

Computer viruses continue their operation after the time of the jamming transmission. This allows for considerably extended effects in comparison with traditional ECM, whose effects begin and end with the jamming transmission. This characteristic considerably extends the vulnerability time of the victim system, allowing the jammer increased accessibility to the victim. Another benefit of this characteristic is that jamming targets can be attacked in advance of the tactical operations they support, thus removing an element of uncertainty in operations planning.

Computer viruses are contagious. They can spread from system to system and from user to user. Once implanted into an initial victim, the effects of computer virus will spread to large groups of users and may have effects considerably more extensive than than the original jamming target. Additionally, this characteristic allows victims to be *indirectly targeted* through intermediate victims. In assessing the vulnerability of electronic systems to EW, consideration is typically given to the system's accessibility to a threat. Based upon this exposure, an appropriate level of ECCM is determined. Through the contagious property, computer viruses can initially attack the weakest element in an enemy's defense, and then provide for subsequent transport to the real target.

Computer Virus EW effects can be precisely tailored. They can be programmed to seek out specific victim systems and once there lie dormant until triggered into action. Examples of effects include surreptitious changes in system functions, system shutdown, destruction of data files and tactical programs.

Computer viruses can be covert. They can propagate and act with the victim user unaware of their presence. Thus they can achieve the ultimate in deception jamming. Denying the victim awareness of the jamming will prevent him from responding either operationally or to counter the jamming. This will cause him to accept as fact the false situation that has been created for him.

ECM Technique Requirements

For computer viruses to play a useful EW role, they must be able to be reliably employed for a designated purpose as part of a specific operation. Experience with EW has shown that the random, uncontrolled use of ECM merely for harassment is of little operational value in comparison with the expended assets.

Planning for a specific purpose. To be a contributor to a tactical operation, the use of ECM must be part of the operations plan. Computer virus characteristics allow for an unprecedented degree of tailoring and timing of computer virus effects. Computer viruses can be created for a variety of pre-planned actions, and can even be coupled into a victim system to lie dormant until called upon for a designated mission. The degree to which this can be accomplished will be limited primarily by the availability of known data on the victim systems.

Reliable employment. The characteristics of computer viruses allow for exceptional reliability in comparison with conventional ECM. Computer viruses attacking victim digital processors will propagate through these processors, and can await triggering of their destructive and disruptive effects. Computer virus effects can be developed and tested in advance of mission requirements.

Effects Assessment. With EW included as part of the operations plan, the tactical commander needs an EW effects assessment as part of his feedback during mission execution. This effects assessment is important to support the decision to continue the plan or to switch to alternate plans. Computer Virus EW techniques can be programmed to provide unambiguous detectable indications that the computer virus is in place and ready to be triggered. This feedback can be obtained by monitoring the victim data links or systems to observe their disruption, or through programmed acknowledgements from the virus program.

Feasibility Factors

Several recent trends in military electronic systems have contributed to the increased viability of computer virus in EW. These include increased use of:

- *Distributed digital processing,*
- *Reprogrammable embedded computers,*
- *Networked communications,*
- *Computer standardization,*
- *Software standardization,*
- *Standard message formats, and*
- *Standard data links.*

Distributed digital processing: The performance capabilities added to military electronic systems by distributed use of digital computers has made their use increasingly attractive. Combined with these performance benefits, the increased availability of computer components such as microprocessors, memory chips, and multiplexer chips has reduced the cost of these capabilities to the point where they are less expensive than simpler uncomputerized designs. These distributed digital processing systems provide the media for computer viruses to operate.

Reprogrammable embedded computers: An additional benefit of computerized designs has been the ability to update functions and capabilities through reprogramming. The increased availability and capacity of reprogrammable memory technologies has simplified the use of these designs. Since a victim system's computer is required as a target of computer viruses, they can only be employed against such systems.

Networked communications: The spread of computer-controlled military electronic systems has increased the need for these systems to exchange data and programs. This has led to increased demand for data communications among computers. Networked communications provide an important media for the rapid propagation and proliferation of virus programs. Additionally, a virus program can attack a system by simply rerouting data exchanges to prevent them from getting to their intended recipient. In other cases, the network itself can be the target of the virus program. Computer viruses have demonstrated their effectiveness in shutting down computer networks.

Computer standardization: The increased use of computer in military systems has created the need for standardization to reduce the acquisition cost and to improve the supportability of these sophisticated systems.

Similarly, establishing standard computer architectures and instruction sets creates families of compatible equipments. The use of standard computer hardware is an important factor in the feasibility of computer viruses in EW, since virus programs must be specifically written for individual computer designs.

Software standardization: With the establishment of standard computer hardware, the selection of software standards for operating systems and programs is a natural next step in reducing acquisition and support costs. As software becomes a significant part of these systems, it cannot be ignored in developing and operating these systems, especially when its success in achieving performance becomes a driver in the management of acquisition programs. The use of standards reduces acquisition risk, provides economies in software development, and allows for software transportability. Since virus programs attach themselves to other programs, the use of software standards will allow the existence of standard computer virus programs for EW.

Standard message formats: The use of formatted message protocols and structures has been shown to improve the effectiveness of data communications while reducing bandwidth requirements. With efficient format design, actual data transport can be reduced to about half of what would otherwise be required. These standard formats greatly simplify the design of tailored computer viruses, since the amount of destructive processing accomplished can be leveraged by attacking formatted information. For example, by simply changing the format identifier in the header of a message, a virus program can make the subsequently transmitted block data

Standard data links: As military systems have placed increased reliance on data exchange, it has been necessary to establish standard data links to provide connectivity among users within efficient spectrum utilization. These data links employ standard transmission and routing protocols, and modulations. To use of these standards may provide a standard entrance point for computer viruses. Alternatively, since many of these data links are controlled by computers, the link controllers themselves may become standard targets.

Coupling Mechanisms

One of the more challenging aspects of developing and employing computer viruses in EW is the ability to effectively implant the virus in the target. To be effective the computer viruses must be placed so that it can propagate and infect the system. Most advanced military C^{3}I systems have protective schemes to defeat enemy interference. Computer viruses possess unique characteristics that can be exploited to circumvent a majority of these protective schemes. Potentially the most useful characteristics of computer viruses used for EW are that:

- *The effects of the virus continue after the source has been turned off, and*

- *Viruses propagate from system to system.*

Using these characteristics there are four fundamental mechanisms by which computer viruses can enter enemy systems: front and back door coupling, and direct and indirect coupling.

Front door coupling. Front door coupling is defined as accessing the target by using media for which the system was designed. For example, front door coupling to an ordinary tactical radio would use electromagnetic waves directed at the antenna and receiver electronics. For C^3I systems the main direct coupling mechanisms would be data and control links. To directly couple with a target, A jamming system would inject the virus directly into the target receiver in attempt to cause the receiver to process and thus implant the virus. The virus would then spread to all systems connected with the infected system. Although penetrating the protective schemes of most C^3I systems would be very difficult, the Computer Virus EW system must only be able to couple with the system in its least protected mode. This phenomenon results from the characteristic that viruses continues to be effective after the jamming transmission. Many electronic counter-countermeasures are designed to react to jamming or other interfering waveforms. When jamming is detected the receiver increases coding or implements other techniques to limit the coupling of the interfering signal with the receiver. Electronic countermeasures are effective only as long as it can overcome the ECCM of the receiver. A jamming system utilizing computer viruses , in contrast, must only overcome computer virus protective measures one time. Once the virus has been implanted, a mode change will not affect the effectiveness of the virus. Basically, *Computer viruses can attack the weakest link in the target's defenses while traditional ECM must be able to defeat the strongest link in the receiver's defenses*.

Back Door Coupling. Back door coupling is defined as any technique used to access the target system by media other than the one for which the system was designed. There are several subsystems through which a jamming system utilizing computer viruses could access a targeted system including:

- *Electronic Power systems*
- *Stability systems*
- *Thermal control systems*
- *Propulsion systems*
- *System structure*

These systems have either direct or indirect electrical coupling to system processors. One approach that has been proposed is to inject viruses via carefully controlled electromagnetic spikes into the target system. Other back door coupling techniques include component design tampering and other forms of espionage. Component design tampering could be used to take advantage of the almost blind replication of western processors into hostile systems. By leaking design characteristics of an infected processor of other component, the enemy may unknowingly place a virus into his systems.

In addition to front and back door coupling, A jamming system utilizing computer viruses can couple with target systems directly or indirectly by exploiting the contagious nature of viruses.

Direct Coupling. The most straightforward, but not always the easiest, way to couple a virus with a target processor is to inject the virus directly into the target system. This could be accomplished by a continuous transmission of the virus code at the same time that the victim receiver is receiving a valid transmission with the objective that at some point in the transmission, the virus code will find its way into the receiver intermixed with the intended transmission. This approach ensures that the virus is at a minimum trying to infect the correct system. The disadvantage is that the target itself may not be the weakest link in the system defense. If the target is a high value system, it may have sophisticated protection schemes to prevent coupling to enemy signals. In these cases, indirect coupling would provide a better mechanism.

Indirect Coupling. One of the most compelling mechanisms for using computer viruses as part of a jamming technique is the process of indirect coupling. Indirect coupling takes advantage of the contagious properties of viruses. The concept underlying indirect coupling is to inject the virus at the most accessible or unprotected point (the initial target) that could eventually spread the virus to the objective target. This virus could be spread from the initial target to the objective target in several ways. One of these ways is illustrated in Figure 1. An EW system is depicted electronically injecting a computer virus into a digital tactical data link where it is received by a tactical aircraft. This virus propagates into the tactical data link through a Command & Control Aircraft and down to a Command & Control Facility. This Facility is linked by land lines to an Air Defense System, which could be attacked by the virus. This virus could be programmed to negate missile launch commands. The presence of this virus would otherwise be unknown to the operators of the targeted system.

Another technique for passing viruses from the initial target to the objective target is through maintenance and diagnostic tools. Processors are commonly checked by diagnostic tools as part of routine maintenance. When diagnostics are run on an infected processor, the virus is spread to the diagnostic tool. Every processor that is diagnosed by the tool after it has been infected becomes infected also. Creating viruses that could be spread in this way is very straightforward.

Propagation is a unique characteristic of computer viruses. Because conventional jamming systems do not have a comparable quality, today's C^3I systems are not designed to counter the effects of propagation. Most current systems are designed against traditional threats that are only effective by direct coupling. Highly protected critical C^3I nodes may be vulnerable to propagating countermeasures simply because they at some point and time connect to unprotected nodes. Whereas with non-propagating countermeasures a node is secure if all links to that node are secure, with propagating countermeasures all links or other devices that have any eventual contact with the node must be protected. The advent of propagating countermeasures creates new opportunities for exploiting enemy network structures and also creates new concerns about friendly security.

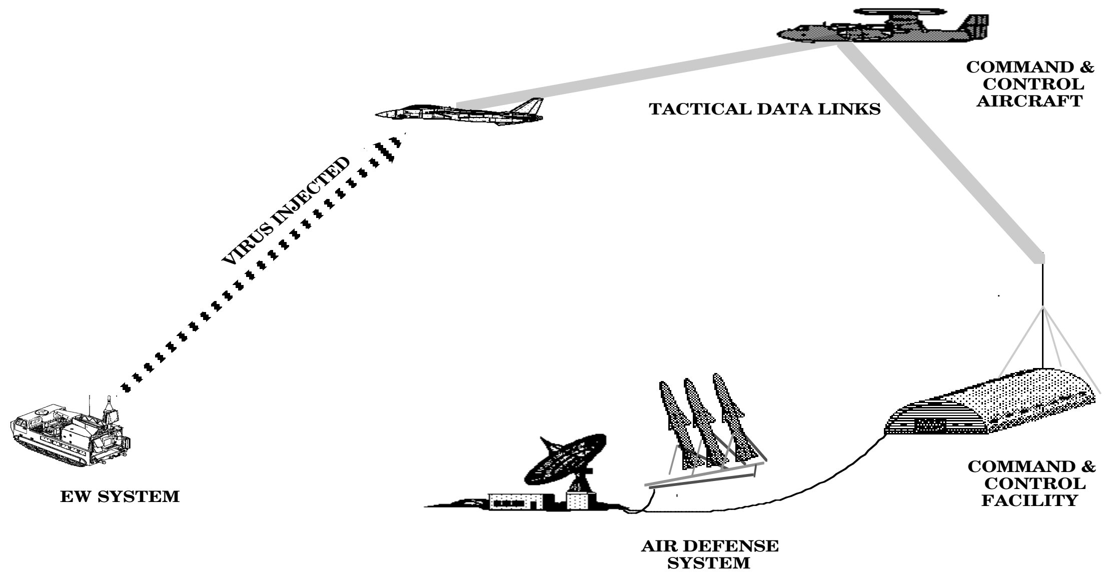

Figure 1. Indirect Targeting

Computer Virus Jamming Strategies

Computer viruses may employed within several jamming strategies, as are discussed below.

Trojan Horse Strategy. The Trojan Horse strategy is just what the name implies. The virus is injected into the target system and lies dormant until a pre-assigned event or time and then it causes catastrophic damage or deception to the system or network in which it resides. The advantages of this strategy are that the virus has no effect until a desired event occurs so it does not raise suspicions. This strategy relies on the element of surprise.

Forced Quarantine Strategy. The Forced Quarantine strategy would be used to target networks. The virus would enter a net and announce itself. The network node would be forced to disconnect itself from the rest of the network in fear of infecting the other nodes. This would force networks to operate as independent nodes, greatly reducing their effectiveness.

Overload Strategy. The Overload virus would simply duplicate itself many times to slow the processing speed of the system. This added delay in the processor may be a tremendous degradation in time sensitive systems such as fire control radars.

Probe Strategy. The Probe virus would search for a specific piece of data and then transmit itself back to a specified location. This would allow highly targeted exploitation for critical pieces of information.

Assassin Strategy. Finally, the Assassin virus would be injected in a network to destroy one particular file, system or other entity. The assassin virus would propagate and then erase itself in all locations until it found the target. The virus would then disable the target and erase itself one final time, leaving no trail.

System Examples

The following two are examples of the types of system trends that create opportunities for Computer Virus EW.

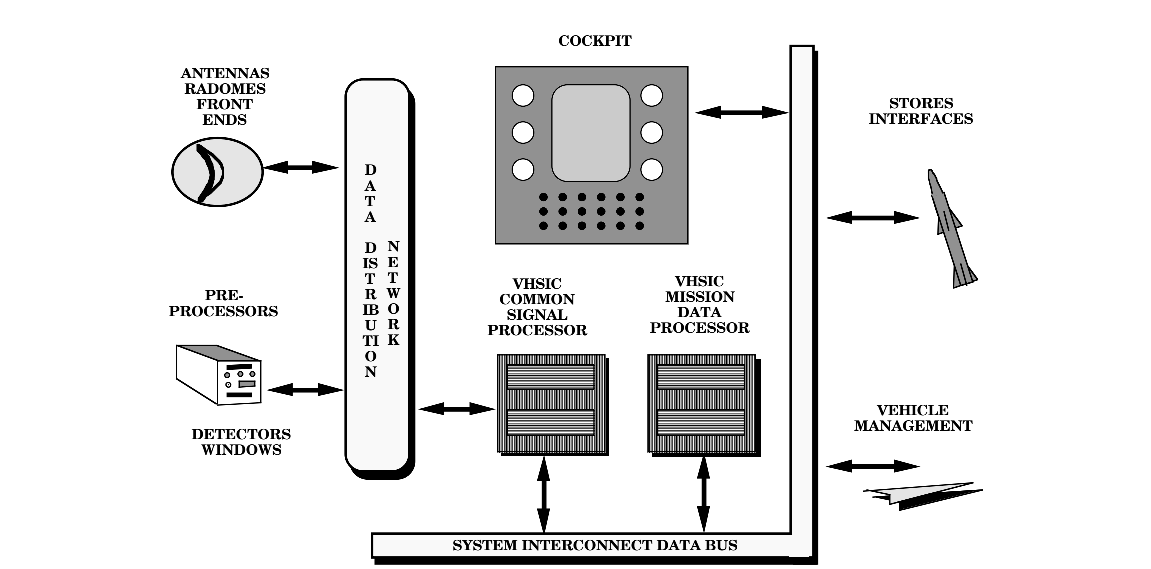
COCKPIT
ANTENNAS RADOMES FRONT ENDS
STORES INTERFACES
DATA DISTRIBUTION NETWORK
PRE-PROCESSORS
VHSIC COMMON SIGNAL PROCESSOR
VHSIC MISSION DATA PROCESSOR
DETECTORS WINDOWS
VEHICLE MANAGEMENT
SYSTEM INTERCONNECT DATA BUS

Figure 2. Advanced Avionics Architecture

Advanced Avionics Architectures. Advanced avionic architectures currently being designed carry forward a development history of increased digital design and functional integration and increased commonality. Vietnam era avionics were characterized by discrete subsystems, some digital and some of analog, consisting of individual electronic boxes. Current generation equipments consist of discrete subsystems, almost all of digital electronic design, still individually packaged, but now interfaced through multiplexed high speed data buses. Developments in support of advanced avionic architectures now are based upon a single avionics subsystem with modular packaging and integrated functions implemented to a great extent in embedded software, supported by high speed data busses. The features of this architecture are illustrated in Figure 2 .

Integrated Command and Control Systems. As advanced weapon systems increase their demands for timely data, complex communication networks have been developing to transport and provide this data to many users including tactical forces, as well as joint and unified forces. Figure 3 illustrates how the Army plans to integrate communications among the maneuver control, fire support, air defense, intelligence/electronic warfare, and combat service support battlefield functional areas. This concept calls for modernization of the Army's communications to provide improved functional connectivity. Key elements in these plans is the use of common hardware and software the use of commercially available non developmental items.

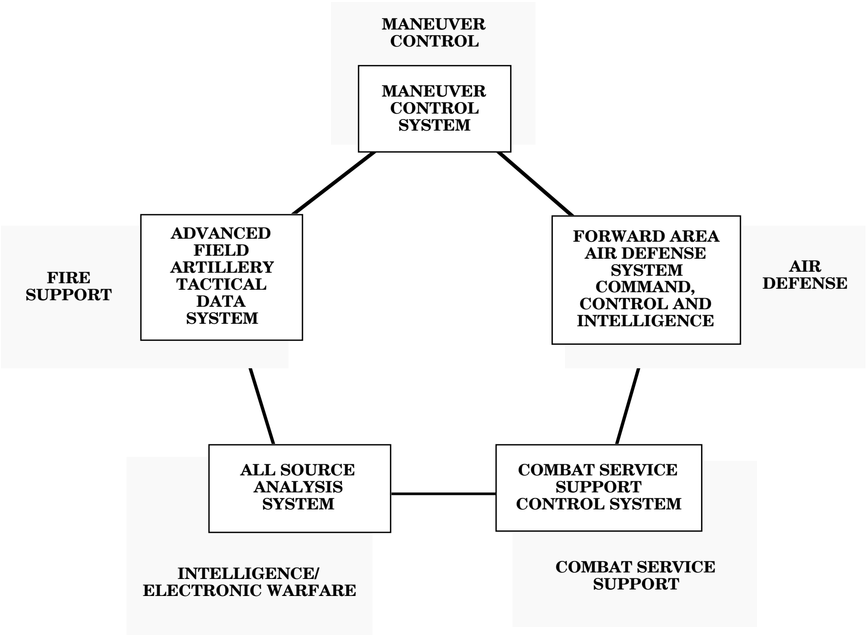
MANEUVER CONTROL
MANEUVER CONTROL SYSTEM
FIRE SUPPORT
ADVANCED FIELD ARTILLERY TACTICAL DATA SYSTEM
FORWARD AREA AIR DEFENSE SYSTEM COMMAND, CONTROL AND INTELLIGENCE
AIR DEFENSE
ALL SOURCE ANALYSIS SYSTEM
COMBAT SERVICE SUPPORT CONTROL SYSTEM
INTELLIGENCE/ ELECTRONIC WARFARE
COMBAT SERVICE SUPPORT

Figure 3. Army Tactical Command and Control System

Protection

Computer Virus EW introduces a wide variety of targets to enemy forces. We must understand the protection requirements, strategy and available techniques to devise an effective protection scheme.

Requirements. Protecting against Computer Virus EW attacks requires significantly more subtlety than protecting against conventional ECM. Protecting a critical node during hostilities requires protection for the links directly connected to that critical node. Protecting these links against computer viruses additionally requires that all links in the critical node's network must be protected against computer viruses not only during times of hostility, but at *all* time prior. In addition, multimode protection schemes such as those used to protect against conventional jamming will only be as effective as the *least-protected* mode. This results because computer viruses can be implanted during normal operations and still be effective during hostilities. Protection must be provided for direct links to the critical node as well as for all other links during normal operations and hostilities. The variety of targets available to hostile forces presents a grim picture if proper protective techniques are not employed.

Protection Strategy. An effective computer virus protection strategy will include several defensive tiers. We recommend a layered strategy consisting of the following six levels:

Level I - ***Deny Access***. This is the first protection layer and includes measures to keep intruder software out of the system.

Level II - ***Detect***. Recognizing, that it may not always be possible to stop computer viruses from entering systems, the next step involves detecting the presence of the virus programs.

Level III - Contain. An essential element of virus programs is their ability to propagate within an infected system; accordingly, it is important to stop this spread through containment measures designed to isolate the infection from the uninfected portions of the system.

Level IV - ***Eradicate***. Given that virus programs may eventually penetrate a system's outer defensive layers, it is important to have some remedies available to remove the unwanted virus code before significant damage is done.

Level V - Recover. For the occasion when virus programs do cause significant damage to data files or programs before they are eradicated, it is prudent to provide an efficient way to recover these files from up-to-date back-ups as an additional level of protection.

Level VI - Provide Alternative Operations. There may times when technological solutions are either unavailable or come too late. This may be the case for especially sophisticated virus programs which may strike an unaware user. For these instances, operations planning should anticipate this possibility an provide for an alternate plan of operations without the disabled systems.

The first and most desirable step for protecting against computer virus attacks is to deny access to viruses. Barring this, the next option is to detect the virus once it has gained access. Virus detection is a critical step to protecting systems. Many viruses are difficult to detect and can evade simple detection schemes. Virus containment is the next critical step. Once the virus has been contained, it can be eradicated and recovery can begin. If the virus is not able to be contained, contingency plans must be initiated.

Techniques. Implementing an effective protection strategy against computer viruses requires effective hardware and software design as well as disciplined operations. Table 2 summarizes several alternative techniques for implementing an effective protection strategy.

Table 2. Protection Options

	HARDWARE	**SOFTWARE**	**OPERATIONS**
I Deny Access	ROM PROM CD	Screening Programs Immunization Programs	Physical Security Encryption
II Detect		Monitoring Programs	System Activity Observation
III Contain	Physical Isolation Multiple Processors	Multiple Operating Systems	Physical Security Quarantine of infected users
IV Eradicate		Virus Removal Software	File Configuration Management
V Recover	Backup & Restore Software	File Configuration Management	
VI Alternate Operation			Contingency Planning

Hardware

- *Use PROMs, CDs or other Read-Only Memory to deny access to executable software programs.*
- *Electrically isolate systems to contain spreading viruses.*
- *Integrate a variety of different multiple processor types to contain spreading viruses by denying them their media. To be effective in this environment, a virus program would have to simultaneously work within each microprocessor's instruction set.*

Software

- *Screen programs to deny programs performing unauthorized functions access to CPUs.*
- *Use immunization programs to build in software protection into system software, thus denying the virus access to the programs it would otherwise infect.*
- *Monitor programs to detect viruses.*

- *Integrate multiple operating systems to contain spreading viruses. To be effective in this environment, a virus program would have to simultaneously speak the language of each system.*
- *Use anti-viral programs to eradicate viruses. These programs would process the infected code, and surgically delete the virus programs.*
- *Reload software to recover from virus. This approach involves simply erasing the infected programs and files and reinstalling them from clean copies. In Many instances this many be simpler than trying to eradicate viruses from individual programs.*

Operations

- *Initiate disciplined OPSEC and INFOSEC to minimize the system's exposure to virus programs and to limit access to critical system elements. Part of this involves anticipating possible routes of virus infection or propagation and blocking these.*
- *Observe system activity to detect viruses. The best protection tools are ineffective if they are not used in a timely and consistent manner. The best protection is timely detection.*
- *Initiate strict OPSEC to contain spreading viruses. operational procedures can be designed to limit to spread of virus programs even if they are able to enter a system.*
- *Quarantine infected users to contain spreading viruses.*
- *Develop contingency plans if virus causes catastrophic damage.*

In designing protection for any application, tradeoffs should be made of the costs of incorporating protection compared with the vulnerability and potential for loss that could be realized. Additionally, a system's acquisition status will be a factor in constraining the available options. This is summarized in Table 3. Although all options at all levels may be open for conceptual systems, operational procedures may be the only feasible protection option for fielded systems within existing architectures.

Table 3. Protection Options			
	Existing System NEAR TERM	Unfielded System MID-TERM	New Architecture FAR TERM
Architecture	Fixed	Fixed	*Flexible*
System	Fixed	*Somewhat Flexible*	*Flexible*
Sub-system	Fixed	*Flexible*	*Flexible*
Component	Fixed	*Flexible*	*Flexible*
Operations	*Somewhat Flexible*	*Flexible*	*Flexible*

Summary

The destructive potential of computer viruses has been demonstrated by events of recent years. The capabilities of these programs against computer systems and networks must be taken into account in the design of current day commercial communications and computer systems and operations.

Current trends in the development of military electronic systems, while beneficial from many other perspectives, have unfortunately increased the vulnerability of these systems to computer virus attack. This has created a new form of electronic warfare utilizing computer viruses.

Historically, protection schemes against new countermeasure techniques have been integrated into our C^3I structure as a reaction to an operational event that has dramatically affected our capabilities. Such an integration strategy could prove catastrophic against computer viruses. Because viruses can lie dormant among millions of lines of code and then spring up at a critical time, protective schemes against computer viruses must be initiated before an adversary can employ such viruses. It is the authors' estimate that this time may not be very far in the future.

References

1. Ross M. Greenberg, "Know Thy Viral Enemy", *Byte*, June 1989
2. Susan Kellam, "Adapso Urges Congress to Act on Viruses", *Washington Technology*, July 13, 1989
3. Gen Louis C. Wagner, "Modernizing the Army's C3I", *Signal*, January 1989
4. U.S. Air Force, *Architecture Specification for Pave Pillar Avionics*, Specification SPA90099001A, January 1987
5. Lance J. Hoffman, *Rogue Programs: Viruses, Worms, and Trojan Horses, 1990*
6. Ralf Burger, *Computer Viruses. A High Tech Disease,* 1988