STRATEGY
RESEARCH
PROJECT

The views expressed in this paper are those of the author and do not necessarily reflect the views of the Department of Defense or any of its agencies. This document may not be released for open publication until it has been cleared by the appropriate military service or government agency.

VIRUSES AND OTHER COMPUTER PATHOGENS: SHOULD DOD CARE?

BY

LIEUTENANT COLONEL (P) ROBERT A. KIRSCH II
United States Army

<u>DISTRIBUTION STATEMENT A:</u>
Approved for public release.
Distribution is unlimited.

USAWC CLASS OF 1997

U.S. ARMY WAR COLLEGE, CARLISLE BARRACKS, PA 17013-5050

USAWC STRATEGY RESEARCH PROJECT

VIRUSES AND OTHER COMPUTER PATHOGENS: SHOULD DOD CARE?

by

LTC(P) Robert A. Kirsch II
United States Army

Professor Steven Metz
Project Advisor

U.S. Army War College
Carlisle Barracks, Pennsylvania 17013

The views expressed in this paper are those of the author and do not necessarily reflect the views of the Department of Defense or any of its agencies. This document may not be released for open publication until it has been cleared by the appropriate military service or government agency

ABSTRACT

AUTHOR: Robert A. Kirsch II (LTC(P), USA

TITLE: Viruses And Other Computer Pathogens: Should DoD Care?

FORMAT: Strategy Research Project

DATE: 1 April 1997 PAGES: 25 CLASSIFICATION: Unclassified

Information technology -- computers, networks and their associated software and communications -- has been evolving at an astounding rate. Viruses and other computer pathogens, which have existed only for a few years, have been evolving at an equally high rate. We must now acknowledge the potential for more aggressive virus attacks which can wreak significant strategic damage. Military and civilian administrative and logistic computer and communications systems represent the most lucrative potential targets. Tactical systems generally are closed; their operating systems have not yet been attacked, since they communicate and transfer data over non-public, tactical and strategic communications systems. However, the potential for attack by a determined person or persons exists. This threat will increase as we become more dependent on these strategic systems. The time has come to anticipate how, by whom, and under what conditions an attack will occur. Computer pathogens have matured to a state where no computer system is completely safe, unless it is stand-alone. Computer viruses avoid detection by constantly changing their identity; network worms can gain access to most networks; and Trojan Horses can do both without the user's knowledge. Once the pathogens are present and a triggering event occurs, the potential damage they may do is incalculable. If DOD intends to rely on its strategic systems in the future, it must plan for and deal with viruses and other computer pathogens now.

TABLE OF CONTENTS

INTRODUCTION

The tactical and strategic command, control and communications systems of today's Army are becoming more and more dependent upon automation. Likewise, America's commercial strategic systems, utilities, communications networks, and financial networks are increasingly dependent on computers. As a result of this increased automation, all of these systems are becoming more vulnerable to attack. This threat does not come from physical attack from bombs or artillery shells, although physical attack is always a concern. Rather, it comes from computer viruses. Generally, a virus is one of group of computer pathogens made up of viruses, worms and Trojan horses. This study discusses each of these threats, although viruses will be addressed in more detail since they pose the most insidious threat.

Consider the following scenario: At exactly 0530 hours on some date in the future the server nodes of the Secure Internet Protocol/Routing Network (SIPRNET), Non-Secure Internet Protocol/Routing Network (NIPRNET) and Tactical Internet (TI) begin to fail. In less than 30 minutes dependent organizations have totally lost the ability to move position reports, OPORDs, data, and communications. At exactly 0600 hours that same day, a near peer adversary attacks a number of U.S. installations and tactical positions. Initially, we are unable to communicate, pass on the tactical or strategic picture of the battlefield, or coordinate fires. Eventually, the networks are restored and we are able to overcome the attack, but only after great loss of personnel and equipment. Impossible, you say? I think not. The introduction of computers into Department of Defense (DoD), in garrison and on the battlefield, and into U.S. society in general has lead to an unprecedented improvement in combat system effectiveness, speed of communications and productivity. It has also led to an unanticipated reliance on them to do everything but make tactical and strategic decisions. As we increase our use of and dependence on computers, our potential adversaries are looking for ways to exploit this ever evolving global information infrastructure.[1] This situation only serves to increase the likelihood that an event such as the one described in the scenario will happen. It is only a matter of when, where and how. Viruses can attack without warning, quickly shutting down systems. For example, consider the October 1996 attack on the Environmental Protection Agency's Mid-Atlantic Regional network.[2] In that case a virus infected more than 600 computer work stations, causing the loss of all of their files. The virus was able to infiltrate three levels of virus protection as it infected the 600 stations.

Why are viruses important? Quite simply, they form a potential class of computer warfare weapons that fall within the domain of Information Warfare. More importantly when national or theater wide cyber space or computer systems are involved, the threat of viruses becomes strategic in nature.[3]

This SRP will discuss the origin of computer pathogens (viruses, worms, and Trojan horses), their types, methods of infection, methods of transmission and probable evolution. It assesses the potential for a strategic computer viruses epidemic and the vulnerability of America's strategic C4I systems.

BACKGROUND/DESCRIPTION

Fred Cohen defines a computer virus as "a computer program that can infect other computer programs by modifying them in such a way as to include a possible evolved, version of itself."[4] Computer viruses are actually a special form of "malicious logic."[5] The existence of computer viruses can be documented as far back as 1981. Then the virus was transmitted between Apple II computer disks as part of the operating system, which was always written to a disk as part of the disk-formatting process.[6] Since their first documented introduction, they have continued to develop and mature. To date, the National Computer Security Association (NCSA) has identified and cataloged over 10,000 computer pathogens and their variants.[7] Of that number, 614 have been identified in the "wild," which means they are currently infecting computer systems somewhere in the world.[8] Numerous types of computers have been targeted for attack by viruses. Currently, almost all computer viruses in the wild target the class of computers called personal computer (PC). The cost and availability of PCs may account for their vulnerability and popularity as targets, as we shall see later.

WHY ARE VIRUSES BEING DEVELOPED

There are over 10,000 known viruses. But why would anyone want to write an application that would potentially cause harm? The first viruse, "Apple Virus 1," was written in 1981. It was written in order to see if a program could be developed that would replicate as a virus does, in the biological sense, for no other reason.[9] However, there have been numerous subsequent examples where the writer intended to do harm -- and did. The first instance of a malicious virus being introduced into the wild was the "Lehigh" virus. This virus would infect the boot track of a disk. There after infecting four other disks, it would overwrite the File Access Table (FAT) and boot track.[10] But David Harley in "Frequently Asked Questions" has some ideas of his own as to why viruses are written: 1) Writers don't understand or prefer not to think about the consequences. 2) They simply don't care. 3) They get a "buzz," acknowledged or otherwise, from such "creative" vandalism. 4) They consider they're fighting authority. 5) They're keeping the antivirus vendors in business.[11] Vesselin Bontchev in "The Bulgarian and Soviet Virus Factories" quotes one virus writer as saying "destroying data is a pleasure." The writer admits that he "just loves to destroy other people's work."[12]

DISCUSSION

The majority of viruses currently in the wild target and infect PCs running the Microsoft Disk Operating System (DOS), Windows, or Windows 95 -- rather than other computer platforms running Digital VMS, UNIX, or mainframe operating systems. PCs are more readily available to the world population as a whole, and the Microsoft's operating system is simple to learn, manipulate and thus break into. PCs are available to everyone; you can buy a PC for as little as a few hundred dollars if are not seeking state-of-the-art hardware.

Just as freedom of speech has allowed some very radical ideas to flourish, ready access to PC has allowed some disgruntled and/or irrational persons to develop software that cause their PC and other people's PCs to do things they where not originally intended to do. This software may, for example, delete files, change data, or reformat a disk without notification or permission. UNIX and Mainframe systems, on the other hand, are more expensive, have tighter operating system security, and are less accessible to the general population as a whole. These factors probably account for the limited number virus sightings in these systems. However, they are certainly not immune to attack. But the development of a virus to target a UNIX or mainframe system will require a concerted effort by a dedicated group that is sponsored by an individual or group of individuals that can afford the appropriate computer resources. In fact, when such viruses are written, they will be designed specifically for the purpose of infecting the target host and destroying it. There is a documented instance of a group of college students in Serbia who have declared that they are developing a UNIX virus, specifically a worm, to attack the nascent Internet.[13]

METHODS OF ATTACK (TYPES OF PATHOGENS)

VIRUS

A virus is a program that attempts to replicate itself in the wild. That is, it attempts make copies of itself on target hosts. Computer viruses are so named because of their functional similarity to biological viruses, in that they can spread rapidly and uncontrollably throughout a host system.[14] For a virus to spread, its code must be executed. This can occur either as the direct result of a user invoking an infected program, or indirectly through the system executing the code as part of the system boot sequence or a background administrative task.[15]

However, computer viruses cannot be transmitted through the air like biological viruses. Nonetheless, they could be transmitted via a wireless modem from one infected system to another, provided an infected file is transmitted. Viruses are categorized and labeled based on how they attempt to avoid detection, how they infect a target host, how quickly they infect a host, and to what degree they infect the host.[16] Developers of computer viruses have contrived some rather unique ways for their viruses to attempt to avoid detection once they have infected a host. They include the Stealth virus, the Companion virus, the Armored virus, and the Polymorphic virus. The Stealth virus will monitor the system it has infected and return false results to systems functions that might identify its presence. The Companion virus will create a new program that will be executed instead of the intended program. The intended program will be run after the virus has been executed. The Armored virus uses special tricks to make the tracing and disassembly of its code more difficult. Finally, the Polymorphic virus is a virus that modifies each copy of itself as it is replicated. In so doing, it alters the signature of the virus which is used by most virus detection programs to identify potential viruses in the a system.[17]

Viruses are further subdivided into those that are memory resident and those that are non-memory resident. Memory resident viruses make themselves resident in a system's memory when an infected program is run; it then infects other files any time they are opened or executed. Non-memory resident viruses are active only when an infected file is executing, but do not remain in resident memory -- they "hit and run". They will only infect files that opened or executed while they are active.[18]

Viruses are also categorized by the method they use to infect the target system. These types of viruses include system or boot-record infectors, file infectors, and file system or cluster infectors. The system/boot record infector places itself in the boot sector of any uninfected disk, either floppy or hard disk. This type of virus can only infect a disk during the system boot process, since this is the only time that this portion of the disk is accessible. If an infected floppy is used to boot the system, the virus will attempt to locate a hard disk on the system to infect. This type of virus is generally of the memory resident variety. The file infector will infect any file that is open or opened during its execution; it may be of the memory or non-memory resident type. Finally, the file system/cluster infector virus will modify the FAT information to cause the virus to be executed whenever the target file is executed. This type of virus is difficult to identify, since a listing or directory of system files will show the name of the target file, not the virus.[19]

The final descriptive classification of viruses identifies how quickly and completely they infect the target system. These classifications are fast infectors, slow infectors, and sparse infectors. The fast infectors will infect all files on a victim system whether they are open or not. The slow infector will infect only files that are opened while the virus is active. The sparse infector will infect only a limited number of files in a given time period, like every tenth file or files opened on the 3rd of each month.[20]

Finally, virus are named based on where the virus was first discovered or where a major infection occurred, such as the Lehigh which was discovered at Lehigh University. "Viruses are also named after some definitive string or value found in the program, such as the Brain and Den Zuk virus, which contained the character string brain and den zuk. Sometimes viruses are named after the number of bytes by which they extend the infected file."[21]

TROJAN HORSE

Trojan horses appear to be legitimate programs, but they have hidden agendas.[22] However, in reality a Trojan horse is intended by its developer to transport a virus or worm to a target platform. This type of pathogen requires the participation of the developer of the cover application.[23] But, this is not always the case. In at least one documented instance, a compiler was modified to add the virus code to log-in scripts that were compiled.[24] The Trojan Horse does exactly what it is suppose to do; but in addition to its publicized function it deposits the malevolent code on the target.

NETWORK WORM

A network worm is an independent program that spreads by making complete copies of itself across a communications network. What makes network worms so dangerous is the number of networks that have gained strategic importance because of their use in the movement of governmental, military, and commercial data. The Advanced Research Projects Agency Network (ARPANET), Military Network

(MILNET), the Non-secure Internet Protocol Network (NIPRNET), and the Secure Internet Protocol Network (SIPRNET), to name but a few, form what is called the INTERNET.[25] Once active within a system, a network worm could behave as a virus. Or it could implant Trojan horse programs or perform other disruptive activities.[26] Generally, worms confine themselves to persistent attempts to replicate. This in and of itself is enough to consume system resources and in most instances will cause the system to crash.[27] Worms usually restrict themselves to the Local Area Networks (LAN) where they can easily obtain password information which is necessary for them to reproduce. However, there are an increasing number of instances where worms have replicated across the Internet. In these cases, the worm generates a Universal Resource Locator (URL) and attempts to establish a File Transfer Protocol (FTP) session. If it is successful, it will FTP itself to the target host and attempt to repeat the process from that host.[28] In another instance, the worm listened for passwords and then establishes a UNIX sendmail session using the purloined password and attempted to replicate itself in this manner.[29]

PSYCHOLOGICAL ATTACK

An adversary need not attack a system directly in order to cause a particular problem. He only has to cause the system user to think that a problem may exist. By so doing, he will achieve his desired goal of work disruption, message traffic interruption, and possible system shut down. This can be accomplished by simply introducing an apparently authentic e-mail message into the system. This message may indicate that a virus, network worm, or Trojan horse has been introduced into the system and recommend a precautionary action.[30]

TARGETS

At first glance the traditional target of a virus seems to be user's systems. That is to say, the virus infects the system; and then at a given point when the virus is triggered, it will perform whatever task the developer intended. During the infection stage the virus will target the file system or operating system of a particular platform. During this stage, the virus tries to replicate itself on the target platform. When the virus is activated, the target will be the file system, the system memory, the system display, system output, or the operating system.

The operating system is what generally gives the platform its name. The most common and most often attacked are IBM and MS DOS, MAC OS, WINDOWS, OS2, WINDOWS 95.[31] Viruses often attack these platforms because their security systems are weak and easily bypassed.

But what about other types of platforms like mainframes, UNIX, and others. It is quite possible to write a virus that will run on and infect mainframes and mini-computers running any operating system.[32] This fact was demonstrated by Professor Fred Cohen while he was a doctoral student at the University of Southern California. He demonstrated that several types of systems (IBM, DEC, Tops-20) could be infected by a virus.[33] A successful strategic attack on a mainframe system is only a matter of time, money and access. This study does not detail mainframe viruses, not because they are not a potential problem, but because they are not used as widely as DOS, WINDOWS, and UNIX platforms are. We have considered the vulnerabilities of DOS and WINDOWS platforms. What about the vulnerability of UNIX platforms?

In order for a virus to infect a UNIX platform, it must have root level privileges. To infect a new file, it must be able to read the file and rewrite it after the virus has infected it. DOS platforms generally run operating systems provided by IBM or Microsoft, while UNIX platforms and the UNIX operating systems are dependent on the particular manufacturer that provided them. The manufacturer will make enhancement to the UNIX OS based on his need. However, all UNIX implementations are generally compliant with the UNIX standard developed by AT&T. A unique security feature of UNIX is that an application's ability to read, write, delete or change a file is based on the rights assigned to the user/owner of the file. These rights are assigned by the system's administrator, who can do anything: In UNIX lingo, he has "root level" privileges. Most importantly, he can create users. In order for a virus to work within a UNIX system, it must first obtain the necessary rights.

There are several ways to obtain these rights. One way would be to monitor the system and obtain userid/password combinations. This could be done by installing an application that would listen for the log-on process and capture the userid/password. This listening technology is commonly called a sniffer. Once a userid/password was been obtained, the virus would attempt to infect the files belonging to that user. This is a tricky process, but not impossible to accomplish. A polymorphic virus would be well suited for this, since it could change its fingerprint continuously and therefore avoid detection. The virus would identify userid/passwords in its sniffer mode and change itself prior to attempting to infect another file. In other words, the father: the original virus, would clone itself using a new userid/password thus creating a son. The father would then attempt to perform the infection process again. The son would wait to be notified by the father of success. If the father was not successful, did not notify the son, the son would repeat the duplication process as its father had prior to attempting to infect files himself. Thus the son would become a father.

A second option would be the identification of hidden OS level capabilities to execute, read, change, write, and delete files. This capability is generally referred to as an OS backdoor.[34] If it exists, it is generally closely guarded. But determined parties could obtain it. A virus that would use this capability would have to be written by an insider or some other informed party, such as a government that supports virus research and development for information warfare purposes. The reason that we have not seen UNIX viruses in the wild is not because they don't exist. It is because once they show themselves the mechanism used to infect will be identified and defenses developed. The question is not whether UNIX viruses will appear, it is when and where they will appear, and how much damage they will wreak.

THE HACKER

The Trojan Horse and Network Worm are difficult method to track because the Trojan Horse looks harmless and the Worm can cover its tracks. The hacker, although not a computer pathogen, is equally dangerous. The dedicated hacker has developed and accumulated a suite of tools and techniques that allow him to gain access to his target system. In most cases, he has developed a routine that he uses when he is attempting to gain access to a new system. He may start by attempting to log in using common account names. He may also attempt to identify active users by using "who," or "finger" common UNIX utilities that identify active users and then attempt to log in using their account names.

If he is lucky, he will gain access on his first try. However, if not successful, he will not give up. He will enlist the aid of a program running on his system that will attempt, over and over, to log in using discovered account names and numerous possible passwords. Once he gains access, he will track down the account name/password file and retrieve it to his own system, where he will use publicly available programs to decrypt the account names and passwords. Or he may install a program called a Sniffer or Trojan Horse that will listen for system log-ons and collect active account name/passwords. The sniffer will then either e-mail the active account name/passwords to him or collect them in a file which he will retrieve at some later date. In any case, he will now be able to install a virus in the hacked system as well as to make further attempts to locate other systems to hack into and infect.[35] So although the hacker may not be as modernistic as the computer pathogen, he is as dangerous and equally worthy of concern.

THE REAL THREAT

The real threat posed by viruses is not that they may infect a host. If all they did was replicate themselves they would be a nuisance -- but nothing more. The real threat is when they become active. They may do nothing more than display of a simple message on the computer screen to annoy the user. But they can do something much more destructive like erase some or all files, destroy the boot track of the disk, delete portions of the OS kernel, cause the disk to be reformatted, or cause the system to crash completely. These destructive acts pose the real threat. Unless the system in question has a good backup, the data which is lost may be irreplaceable. Or the system cannot be restarted. And if the system in question is an accounting system, the user might lose valuable accounting data. If the system is a transportation control system the virus could cause a train wreck. If the system is a financial system a market crash might occur. Or if the system is a critical C4I node, commanders could lose the ability to command and control. Any or all of these will most likely occur that the worst time.

Viruses are being developed all over the world. There are documented cases of viruses coming from foreign countries like Bulgaria, Poland, Russia, Taiwan, and Australia -- to name just a few. Currently, there are no publicly documented cases of state sponsored virus writing. But if the number of viruses is an indication of amateur activity, one can only assume that state sponsored virus development is also taking place.

STRATEGIC QUESTIONS

Viruses thus fall into the broader area of Information Warfare, which is subdivided into netwar and cyberwar according to Arquila and Ronfeldt. They go on to define netwar as information conflict between nations or societies at a grand level, whereas a cyberwar is the conduct of, or preparation to conduct, military operations according to information-related principles that use information and knowledge for strategic benefit. According to Arquile's and Ronfeldt's definition, viruses and other computer pathogens should be considered cyberwar weapons.[36] Molander, Riddle and Wilson in "Strategic Information Warfare: A New Face of War" identified seven defining features of strategic information warfare which clearly suggest that viruses will become the weapon of choice for future conflicts: low entry cost; blurred traditional boundaries; the expanded role of perception management; a new strategic intelligence challenge; formidable tactical warning and attack assessment problems; difficulty of building and sustaining coalitions; and vulnerability of the U.S. homeland.[37] In addition, viruses definitely meet the defining features of strategic information warfare.

So if viruses and computer pathogens are to become the Information Warfare weapons of choice, what kinds of targets will a potential adversary select? Such an adversary will select targets that have the highest potential payoff in terms of shock value and actual loss. He may attack systems that manage the America's infrastructure and financial markets. Then again, he may wait until he is prepared to confront the U.S. on the field of battle and attack our strategic command and control networks.

We have seen how viruses and other computer pathogens are and should be of significant concern. The following questions focus on the strategic threats posed by viruses and other computer pathogens:

1. *Who might use viruses as a tool of war?*
2. *Under what conditions might they be used?*
3. *How might they be employed?*
4. *What should we do?*
5. *What is the appropriate response?*

Who might use viruses as a tool of war?

There is an ever expanding group of potential users of viruses. They can be divided into the following general groups: hackers, non-state actors, and state actors. Hackers include those individuals who develop and disseminate viruses for personal generally non-political reasons. They include high school and college amateur programmers, as well as professional programmers who have a personal ax to grind. The non-state actors include criminals, narco-terrorists, and political terrorists. The criminal and narco-terrorists may utilize viruses to extort money or desired actions from target groups. Political terrorists may utilize viruses to advance their particular political goals.

Why are these groups of potential users of viruses for strategic purposes expanding? Viruses are relatively cheap to develop compared to other strategic weapons and the strategic targets that are susceptible to them are extremely lucrative. A potential user need only obtain the services of an accomplished and willing programmer and a representative example of the target platform for development and testing. In a short while and with a small investment, the potential adversary will have a strategic IW weapon.

Under what conditions might they be used?

Several circumstances might cause an actor to consider using viruses to achieve certain goals. And criminal elements may desire to extort money from financial organizations or other businesses. Consider the fictional case of the Japanese business tycoon who causes a computer virus to be placed in the code of the Dow Jones stock transaction tracking system.[38] On the other hand, a narco-terrorist may attempt to force some action or inaction on the part of a law enforcement activity or a government agency, or he may seek to wreak some retribution for perceived past legal harassment in the form of arrests or seizures of narcotics in shipment.

The state actor is perhaps the most dangerous and therefore should be of the greatest concern. The state actor may use viruses for some of the same reasons that a non-state actor does: to harass, extort money, force a course of action, or extract retribution. They will also surely plan on and quite possibly use viruses for preparation of the battlefield. They will cause command and control systems, communication switching systems, and logistics systems to be infected with a virus or other computer pathogen and then triggered at a time and place of their choosing -- most likely in conjunction with a ground, air, or sea attack. Of course these actors will only succeed if the U.S. remains vulnerable to strategic virus attack.

How might they be employed?

First and foremost, all strategic systems should be evaluated for their vulnerability to attack. We must develop a methodology that will allow users to determine those system level weaknesses that could be exploited by an actor bent on infecting our strategic systems, prior to an actual infection. This methodology should address system access, operating system architecture and vulnerability, data movement between systems, and access to administrator level (root) rights. Next, we should develop a plan of action that addresses any short-comings that are identified. Immediate action should be taken to insure that access to root level rights are restricted and proper backup procedures are being followed. Finally, offensive counter-measures must be developed. The particular organization that should have this mission is a subject worthy of considerable discussion. However, for the sake of brevity, the organization should have the ability to operate independently, be able to perform both offensive and defensive IW, and answer directly to the National Command Authority (NCA). In short, it should be an organization that is at the Commander in Chief (CINC) level, if not in fact a separate CINC IW.

What should we do?

Suppose we are successful in identifying systemic virus risks, putting together a plan of action to anticipate potential attacks, and developing tools and techniques to counter potential attack. Will we then be able to coordinate and execute effective countermeasures? If the current fragmented and disjointed approach to counter-virus/Information warfare is maintained, we probably will not be able to defend ourselves. There must be a single CINC level authority responsible for risk assessment, plan development, and execution for the military and civilian sectors, both for defensive and offensive operations. This single authority must be able to martial and direct all available resources, if we are going to prevent, stop, or react effectively to potential or actual virus attacks.

What is the appropriate response?

The appropriate response to a strategic virus attack is to consider it an attack on the United States proper. Therefore, it is an act of war. As such, it should warrant a conventional attack at least as destructive as it was. Additionally, we should have available our own suite of offensive virus capabilities to be used in retaliation when justified -- and preemptively when necessary.

CONCLUSION

Virtually every strategic system is vulnerable to virus attack. Those systems that use the Internet for interconnectivity are especially vulnerable. The only way to be 100% sure that a system will not be come infected is to operate in a stand alone mode. This may be possible for some kinds of systems, but impractical for almost all DOD command and control, logistics, financial and data retrieval systems, as they gain their utility from being interconnected. In light of this fact and the information previously presented, DOD has every obligation to be extremely concerned about computer viruses.

RECOMMENDATION

DOD should take immediate steps to designate a single responsible authority to: identify potential strategic automation targets, assess their venerability, and implement defensive and offensive IW programs that will insure that our strategic systems are effectively protected from external intrusion and infection from foreign viruses and other computer pathogens.

ENDNOTES

[1] Roger C. Molander, Andrew S. Riddle, and Peter A. Wilson, "Strategic Information Warfare A New Face of War," Parameters 26 (Autumn 1996): 81.

[2] Elana. Varon, "Virus prompts partial EPA shutdown." Federal Computer Week, 11 November 1996, 6.

[3] Roger C. Molander, Andrew S. Riddle, and Peter A. Wilson, "Strategic Information Warfare A New Face of War," Parameters 26 (Autumn 1996): 83.

[4] Fred Cohen, "Computer Viruses" Ph.D. Dissertation. Pittsburg: ASP Press, 1986, 10.

[5] William. Orvis, "The Computer Incident Advisory Capability - Virus Information Update," 1 March 1991, <http://www.bocklabs.wisc.edu/~janda/ciac_b16.html>, 1 September 1995.

[6] Robert M. Slade, "History of Computer Viruses." 10 April 1996, <http://www.bocklabs.wisc.edu/~janda/sladehis.html >, 22 January 1996, 4.

[7] National Computer Security Association, "NCSA Approved rating." 28 February 1997, <http://www.ncsa.com/avpdcert.html>, 3 April 1997.

[8] National Computer Security Association, "NCSA Approved rating." 28 February 1997, <http://www.ncsa.com/wildlist.html>, 3 April 1997.

[9] Robert M. Slade, "History of Computer Viruses." 10 April 1996, <http://www.bocklabs.wisc.edu/~janda/sladehis.html >, 22 January 1996, 4.

[10] Ibid., 5.

[11] David Harley, <d.harley@icrf.icnet.uk>. "Frequently Asked Questions (FAQ) 4/4", 29 November 1996, <alt.comp.virus>. 29 November 1996, 15.

[12] Veselin Gontchev, "The Bulgarian and Soviet Virus Factories." <Http://www.einet.net /galaxy/engine...y/security/david-hull/bulgfact.html>, 13 November 1996, 4.

[13] Chris Hedges, "Serbian Response to Tyranny: Take the Movement to the Webb," 8 December 1996, <http://search.nytimes.com/web/docsroot/library/cyber/week/ 1208yugo.html>. 13 February 1997, 3.

[14] Computer Security Division. "An Abbreviated Bibliography for Computer Viruses and Related Security Issues." <http://csrc.nist.gov/training/readlist.txt>.

[15] Ibid., 34.

[16] "Other Terms for Computer Viruses." <http://www.iscs.nus.sg/~chiayewl/virus/term.html> 13 February 1997.

[17] Ken Van Wjk, "Frequently Asked Questions on VIRUS-L/Comp.virus." <ftp://ftp.cert.org/pub/virus-1/FAQ.virus-l>, 18 November 1992.

[18] A. Wong, "Types of viruses"Unknown, <http://www.ccs.neu.edu/groups/honors-programs/freshsem/19951996/awong/types.html> 13 February 1997.

[19] Ken. Van Wjk, "Frequently Asked Questions on VIRUS-L/Comp.virus." <ftp://ftp.cert.org/pub/virus-1/FAQ.virus-l>, 18 November 1992.

[20] Ibid.

[21] Ibid., 30.

[22] Ibid., 181.

[23] <http://www.seas.gwu.edu/student/reto/infowar/info-war.html>, 22 February 1997

[24] John P. Wack, and Lisa J. Carnahan, "Computer Viruses and Related threats: A Management Guide." October 90, <http://csrc.nist.gov/nistpubs/sp500166.txt> 4 March 1997, 17.

[25] Peter J. Denning Computer Under Attack Intruders, Worms, and Viruses. New York: ACM Press, 1990, 39-80.

[26] Ibid., 16.

[27] <http://www.seas.gwu.edu/student/reto/infowar/info-war.html>, 22 February 1997.

[28] Peter J. Denning Computer Under Attack Intruders, Worms, and Viruses. New York: ACM Press, 1990, 191.

[29] Gene Spafford, "Updated worm report", 4 November 1988, <http://catless.ncl.ac.uk /risks/7.70.html>, 25 February 1997.

[30] Stephen M.Hardy, "Should we fear the Byte Bomb?" JED, January 1996, 42.

[31] William Orvis, "The Computer Incident Advisory Capability - Virus Information Update." 1 March 1991, <http://www.bocklabs.wisc.edu/~janda/ciac_b16.html>, 1 September 1995, 1.
Ken Van Wjk, "Frequently Asked Questions on VIRUS-L/Comp.virus." <ftp://ftp.cert.org/pub/virus-1/FAQ.virus-l>, 18 November 1992, 28-29
Datafwllows, "First Windows 95 virus found." 5 February 1996, <http://www.datafellows.

[32] Ken Van Wjk, "Frequently Asked Questions on VIRUS-L/Comp.virus." <ftp://ftp.cert.org/pub/virus-1/FAQ.virus-l>, 18 November 1992. P24 1208yugo.html>. 13 February 1997.
Hedges, Chris, "Serbian Response to Tyranny: Take the Movement to the Webb," 8 December 1996, <http://search.nytimes.com/web/docsroot/library/cyber/week/ 1208yugo.html>. 13 February 1997.

[33] Lance J Hoffman, Rogue Programs: Viruses, Worms, and Trojan Horses (New York: Van Nostrand Reinhold, 1990), 5.

[34] Computer Security Division. "An Abbreviated Bibliography for Computer Viruses and Related Security Issues." 19 April 1990, <http://csrc.nist.gov/training/readlist.txt> 4 March 1996.

[35] Ibid., 164-168.

[36] John Arquilla and David Ronfeldt, "Cyberwar is Coming!" Comparative Strategy, 12 (Spring 1993), 144.

[37] Roger C. Molander, Andrew S. Riddle, and Peter A. Wilson, "Strategic Information Warfare A New Face of War," Parameters 26 (Autumn 1996), 86.

[38] Tom Clancy, Debt of Honor (New York: G.P. Putnam's Sons, 1994).

SELECTED BIBLIOGRAPHY

Harley, David. <d.harley@icrf.icnet.uk>. "Frequently Asked Questions (FAQ) 4/4", 29 November 1996, <alt.comp.virus>. 29 November 1996.

Varon, Elana. "Virus prompts partial EPA shutdown." Federal Computer Week 11 November 1996, 6.

Molander, Roger C., Riddle, Andrew S. And Wilson, Peter A. "Strategic Information Warfare A New Face of War," Parameters 26 (Autumn 1996): 81-92.

Williams, Robert H. "Info Warfare Attacks Score in Military's Risk Pantheon," National Defense September 1996: 16-17.

"Bulletin 96-24," Automated Systems Security Incident Support Team, December 12, 1996.

Narknett, Richard J. "Information Warfare and Deterrence," Parameters 26 (Autumn 1996): 93-107.

Hardy, Stephen M. "The New Guerrilla Warfare," Journal of Electronic Defense 19 (September 1996): 46-52.

Kiras, James. "Information Warfare and the Face of Conflict in the Twenty-First Century," Peacekeeping & International Relations 24 July/August 1996: 8-10.

Harley, David. "alt.comp.virus Frequently Asked Questions," 29 November 1996. <http://www.bocklabs.wisc.edu/~janda/acv_faq.html>. 3 December 1996.

Slade, Robert M. < http://www.bocklabs.wisc.edu/~janda/acv_faq.html >, "Viral Morality: A Call for Discussion." [Find again].

Orvis, William. "The Computer Incident Advisory Capability - Virus Information Update." 1 March 1991, <http://www.bocklabs.wisc.edu/~janda/ciac_b16.html>, 1 September 1995.

Van Wjk, Ken. "Frequently Asked Questions on VIRUS-L/Comp.virus." <ftp://ftp.cert.org/pub/virus-1/FAQ.virus-l>, 18 November 1992.

Porter, Darrell. "Michaelangelo Report." 3 March 1992, <http://www.einet.net/galaxy /engine...ogy/security/david-hull/porter.html>. 13 November 1996.

Kuo, Chengi Jimmy. "What's NOT a Virus." 1 April 1996, <http://www. /www.bocklabs.wisc.edu/~janda/notvirus.html>, 22 January 1997.

Yetiser, Tarkan. "Polymorphic Viruses." 1 September 1995, <http://www. /www.bocklabs.wisc.edu/~janda/polymorf.html>, 24 January 1992.

Slade, Robert M. "History of Computer Viruses." 10 April 1996, <http://www.bocklabs.wisc.edu/~janda/sladehis.html >, 22 January 1996.

CSD Web Master. "CSD Microcomputer Support - Virus Protection." 15 November 1995, <gropher://news.unb.ca/00/FAQ/comp/util/news.answers.00451>, 13 November 1996.

"First Windows 95 virus found." 5 February 1996, <http://www.datafellows.com /virus/boza.html>, 13 November 1996.

Martin, John. "WINWORD <MS WORD 6.x> MACRO VIRUSES FAQ." 2 January 1995, <http://www.capital.osshe.edu/network/macro_faq.txt>, 6 November 1996.

Federal Deposit Insurance Corp. Internet Access and Acceptable Uses, Circular 1351.3 Washington :FDIC, 1 September 1996.

Neale, Eriq. "Computer Virus Information and Resources page." 23 October 1996. <http://lipsmac.scs.unt.edu/Virus/index.html>. 6 November 1996.

Neale, Eriq. "Computer Virus Information and Resources page." <http://lipsmac.scs.unt.edu/Virus/what.html>. 13 November 1996.

Neale, Eriq. "Computer Virus Information and Resources page." 23 October 1996. <http://www.unt.edu/UNT/departments...chmarks_html/marapr95/ goodtime.html>. 6 November 1996.

Jones, Les. "Good Times Virus Hoax FAQ." 12 October 1995, <http://www.nsm.smcm.edu/News/GTHoax.html>, 13 November 1996.

Gontchev, Veselin. "The Bulgarian and Soviet Virus Factories." <Http://www.einet.net /galaxy/engine...y/security/david-hull/bulgfact.html>, 13 November 1996.

"Guns'n Roses Polymorphic Engine (GPE)." <http://wavu.datafellows.fi/v-descs/gpe.html> 13 February 1997.

"Two new Linux operating system viruses." <http://wavu.datafellows.fi/vir-info/index.html> 13 February 1997.

Hypponen, Mikko. "Name Bliss, Alias: Linux virus, HLLO.17892." 28 September 1996, <http://wavu.datafellows.fi/v-descs/bliss.html> 13 February 1997.

Hypponen, Mikko. "Name Staog, Alias: Windows 95 virus, HLLO.4744." February 1997, <http://wavu.datafellows.fi/v-descs/staog.html> 13 February 1997.

"Other Terms for Computer Viruses.",<http://www.iscs.nus.sg/~chiayewl/virus/term.html> 13 February 1997.

"Introduction and Definitions of Computer viruses."<http://www.iscs.nus.sg/~chiayewl /virus/intro.html> 13 February 1997.

Gibson, Steve. "Random comments." InfoWorld, 20 April 1992.

"Polymorphic viruses.", <http://ng.netgatenet/~steenkee/virus/virus3-1.html> 13 February 1997.

Arquilla, John and Ronfeldt, David. "Cyberwar is Coming!" Comparative Strategy, 12 Spring 1993 p. 144, 146-147.

Denning, Peter J. Computer Under Attack Intruders, Worms, and Viruses. New York: ACM Press, 1990.

Hoffman, Lance J. Rogue Programs: Viruses, Worms, and Trojan Horses. New York: Van Nostrand Reinhold, 1990.

Cohen, Frederick B. It's Alive!. New York: John Wiley & Sons, Inc.

Computer Security Division. "An Abbreviated Bibliography for Computer Viruses and Related Security Issues." 19 April 1990, <http://csrc.nist.gov/training/readlist.txt> 4 March 1996.

Wack, John P. and Carnahan, Lisa J. "Computer Viruses and Related threats: A Management Guide." October 90, <http://csrc.nist.gov/nistpubs/sp500166.txt> 4 March 1997.

Clancy, Tom. Debt of Honor (New York: G.P. Putnam's Sons, 1994).