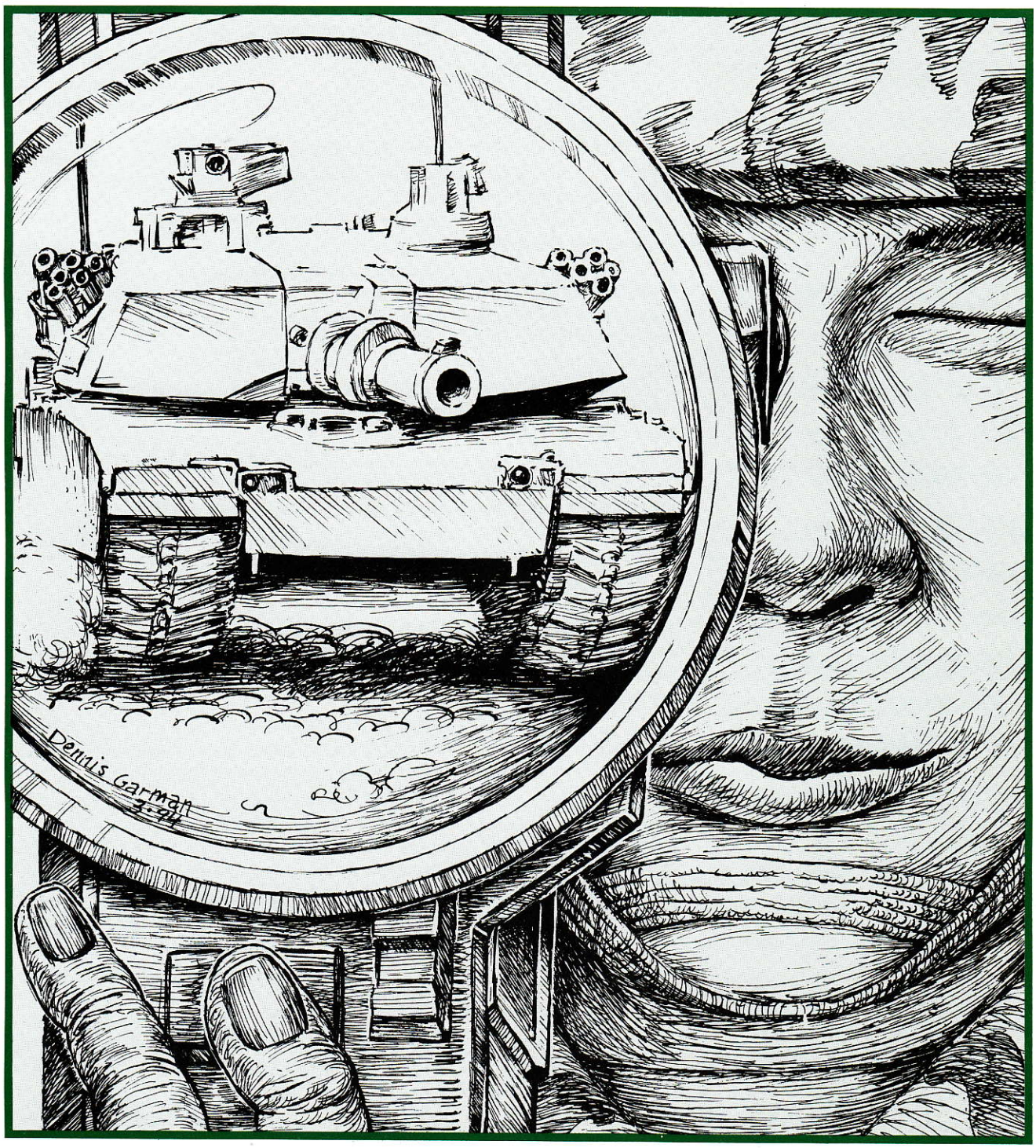
Approved for public release; distribution is unlimited
Headquarters, Department of the Army

PB II-94-1
Spring 1994
Volume 19 Number 1

ARMY COMMUNICATOR

Voice of the Signal Corps



Visual information: a closer look

Illustration by SSG Dennis Garmon

ARMY COMMUNICATOR (ISSN 0362-5745)(USPS 305-407) is an authorized, official quarterly of the US Army Signal Center, Fort Gordon, GA 30905-5301. Second-Class official mail postage paid by Department of the Army(DOD 314) at Augusta, Georgia 30901 and additional mailing offices. POSTMASTER:Send address changes to ARMY COMMUNICATOR, US Army Signal Center, Fort Gordon, GA 30905-5301.
OFFICIAL DISTRIBUTION: ARMY COMMUNICATOR is available to all Signal and Signal related units, including staff agencies and service schools. Written requests for the bulletin should be submitted to Editor, ARMY COMMUNICATOR, US Army Signal Center, Fort Gordon, GA 30905-5301. PRIVATE SUBSCRIPTIONS and rates are available from Superintendent of Documents, US Government Printing Officer, Washington, DC 20402 (202) 275-3015. Fax number is (202) 512-2233. This publication presents professional information, but the views expressed herein are those of the authors, not the Department of Defense or its elements. The content does not necessarily reflect the official US Army position and does not change or supersede any information in other official US Army publications. Use of news items constitutes neither affirmation of their accuracy nor product endorsement. Army Communicator reserves the right to edit material.
CORRESPONDENCE: Address all correspondence to ARMY COMMUNICATOR, US Army Signal Center, Fort Gordon, GA 30905-5301. Telephone DSN 780-7204 or commercial (706) 791-7204. Fax number is (706) 791-3917. Material submitted to publication is subject to editing by the staff. Its mission is to promote the professional development of Army communicators and information mission area (IMA) managers through the dissemination of doctrinal and technical information and the presentation of new ideas/concepts relating to communicators, electronics, automation, printing and publications, visual information and record management. Unless otherwise stated, material does not represent official policy, thinking or endorsement by an agency of the US Army.
This publications contains no advertising. US Government Printing Office:1984-746-045/1429-S. The ARMY COMMUNICATOR is not a copyrighted publication. Individual author's copyrights can be protected by special arrangement. Acceptance by the ARMY COMMUNICATOR conveys the right for subsequent reproduction and use of published material. Credit should be given to the ARMY COMMUNICATOR.

By order of the Secretary of the Army:
GORDON R. SULLIVAN
General, United States Army
Chief of Staff

Official:
PATRICIA P. HICKERSON
Brigadier-General, United States Army
The Adjutant General

ARMY COMMUNICATOR

Voice of the Signal Corps

Table of contents Table of contents Table of Contents Table of Contents

Spring 1994 ***VOL 19 No 1***

Features

2 **A real challenge for the user**
LTC David M. Fiedler (NJARNG) and LTC A. John Purvis (Royal Australian Signals)

7 **The migration to a Global Command and Control System**
MAJ Lorenzo Goins

11 **Improve your office efficiency with a little help from ISDN**
Stephen Larsen

17 **Ada as your first and only programming language**
CPT John C. Norcross

19 **A 40 year old weapon that could compromise US AW**
Raymond J. Lewis

22 **Automated HF communications for nap-of-the earth flying**
James V. Harmon, LTC David M. Fiedler (NJARNG) and LTC John R. Lam (ret.)

27 **Making enlisted personnel management decisions**
Gayle Olszyk

30 **NVIS propagation at low solar flux indices**
Ed Farmer

42 **Visual information: a vital tool for the commander**
CPT Larry Gordon

52 **The additional duty dilemma**
CPT Bernard J. Jansen

Departments

14 Circuit check

48 Signals from the chief

54 TSM notes

A 40 year old weapon that could compromise US AW

by Raymond J. Lewis

The solution to electronic warfare compromise requires a holistic, integrated strategy that includes some engineering, but is mostly doctrine, training, and deterrence.

It's a dream come true for any self-respecting terrorist or small nation dictator: a devastating weapon that's cheap and easy to make. Best of all--from the terrorist's point of view--the United States has no protection against it.

Yes, we know about it, and we could protect ourselves, but we don't. Preposterous? Not at all. It's a concept called automation warfare (AW) that includes computer viruses, worms, Trojan horses, thief programs, hacking, and computer sabotage.

Why is AW important? Because, from a global perspective, all nations look for ways to counter or neutralize the weapons systems or support infrastructure of a hostile nation. A good example is what happened when radio was invented. Armed forces promptly created ways to intercept, jam, and target radio emitters.

Modern warfare depends on a new technology: computers. As they did with radio, armed forces can be expected to develop ways to neutralize computer systems. AW is especially important for three main reasons: our dependency on computers and networking, our vulnerability because our computers and networks have little protection, and the easy availability of AW as a weapon because it's cheap and easily produced.

How dependent are we on computers? Let's look at it from national and battlefield levels. Warfare is a massive societal effort that requires support from many national level agencies and from CONUS logistics. Many details are handled by computer systems.

Our government (including DOD) uses over 900 large computer systems and several hundred thousand small computers (PCs). Nearly half of our large government systems are networked by telephone. Modern telephone systems are actually special purpose computers that connect telephone numbers electronically and are often controlled and repaired remotely.

At tactical levels, telephone switchboards are usually computer controlled and remotely programmed. On the battlefield, tactical computers support complex logistics and personnel actions. Fire direction computers control artillery. In Command Posts, commanders use Army Tactical Command and Control Systems (ATCCS) like the Maneuver Control System (MCS) to gain speed to "turn inside the enemy decision cycle".

Even in peacetime, we are dependent upon ordinary PCs in Army offices.

How vulnerable are we? Too vulnerable. We do little to protect our computers, freely give away information about our computer

systems, and we do not have a systematic training doctrine to teach users how to protect their systems. At national levels, information on many of the larger systems is published in the Federal Register, a public document available to anyone.

Forty-five percent of these large systems are linked by public telephone. Any ambitious terrorist with a modem and a copy of the Federal Register can figure out what to do next.

In fact, a 1990 GAO report found that 8% of the large computer systems were accessed by unknown parties for unknown reasons, and such access is not being stopped.

Looking next at the telephone systems connecting our computers, we find computer controlled telephone switches. Control of the telephone switch is normally done by modem. But telephone dial tone is nothing more than a computer asking "what is your command?".

If one knows the correct codes and has the correct tone device, he can re-program or shut-down an entire telephone switch. Even telephone repairmen doing on-site repairs use dial-up programming to fix problems (Does this sound scary and futuristic? You bet!).

Remember the well publicized January 1990 AT&T telephone black-out of all U.S. long distance capability caused (supposedly) by telephone switch software problems? The same thing could also be done remotely by the AW saboteur to break-down our computer networks.

What about computer systems on the battlefield? How do viruses and saboteurs get to these systems? At first, they couldn't. However, now that we've begun networking our battlefield computers, it is possible for any computer to reach any other computer in the network. As the concept of "Seamless Architecture" progresses at senior leadership levels, we will be networked from national level down to tactical level. We are vulnerable throughout the network because almost every single system is unprotected by hardware, software, or AW trained operators.

How available and widespread is AW? Actually, AW is not new. John Von Nuemann proposed the idea of computer virus-like programs in 1949. Scientists in Bell Labs used to play war games against each other with computer viruses in the 1960s. But the availability and widespread use began when computer viruses were revealed to the public for the first time in 1983. Within a year, **Scientific American** magazine was selling computer virus instructions for only two dollars.

By 1986, an Australian professor, writing in **Futurist** magazine, proposed using computer viruses as weapons against foreign nations, by allowing "pre-infected" technology to be stolen and smuggled into a target nation (This brings to mind those newspaper articles about technology theft by Russia or Iraq). By 1988 viruses began showing up with disturbing frequency all over the world.

Our first real hint of the future came in September 1988. A Cornell University student created a fairly simple "worm" program (a type of virus), dubbed the "Internet Worm", that infected over 6,000 UNIX computers in ARPANET, a network of schools, corporations, DOD, and federal agencies. Even uninfected systems were shut down for fear of infection. A DOD crisis action team even then recognized the threat and recommended establishing a national level agency to cope with AW. But, little was done.

Over the next several years, viruses and hacking compromises into DOD computers increased.

In 1989, a best selling book, **The Cuckoo's Egg** revealed how one computer hacker in Germany used world-wide networks to enter over 400 U.S. Defense Department computers, stealing information at will. Such events often receive huge media coverage, alarm the public, and damage the credibility of the DOD and the U.S. government. Yet we do nothing. Only the Air Force and Navy eventually set up central agencies to cope with AW.

Our next big hint came during Operation Desert Storm. The actual OPLAN was written on a notebook PC that was unprotected and stolen (although later returned). Later, three types of viruses were found on PCs in the theater, though they were removed before tactical computers become infected.

The DOD Security Institute later recognized the seriousness of AW when its 2-91 bulletin specifically pinpointed MCS as a critical and very vulnerable system. Unfortunately, we still didn't heed any of the warning signs.

Finally, in 1992, four MCS systems were rendered ineffective during Exercise Brilliant Diamond due to the DOS "stoned" virus passed by disk and network file transfers.

By now, we shouldn't need more hints. AW is a real threat to our computers.

Unfortunately, AW has many sources: students, ordinary citizens, even public corporations trying to stop competition. There are even "BBS" services devoted to helping such people.

As automation literacy grows, so does the problem, frequency of AW attacks, and our risk. Most people regard AW as a "victimless crime" (like insurance fraud). Coupled with a legal system that normally can't catch perpetrators and won't prosecute them either, there is little to deter AW. And this does not even begin to describe AW caused by foreign sources.

One can easily see that AW has been available and widespread for many, many years.

But there is an even more frightening aspect; the first computer viruses were written in a programming language known as UNIX. When PCs became popular, viruses were written in multi-languages and thus work in UNIX or DOS, wherever the virus code finds itself.

Army garrison PCs operate in DOS, and Army tactical computers (ATCCS) operate in UNIX, and can use DOS as well. This makes Army systems vulnerable from every possible source in existence. So far, AW problems in tactical systems have been caused by using infected DOS diskettes and file transfers. However, we should not need more hints to know that this will change too. If we can have computer inter-operability, we can have virus inter-operability.

In fact, the 1988 Internet Worm carries an even more disturbing implication---that code was written in part using Digital Encryption Standards (DES) technology. There are hints that wireless LAN or WANS might be infected even though the radio system is secured by encryption (AW is a great little cheap, scary weapon, isn't it?).

Of course, I've discussed little of the problems and damage caused by hacking (breaking and entering into a computer) or other aspects of AW. But consider the saboteur. How much easier it is to distribute free infected game disks to soldiers in post towns, knowing that sooner or later some soldier will put an infected disk in an Army computer. Viruses could be easily "pre-planted" and then activated during a conflict.

In tactical systems, a virus does not even have to operate fully to succeed. If the speed or processing of information is sufficiently impeded, the commander has lost the automation combat multiplier and speed advantage. Even a lack of confidence inspired by fear is successful AW if it causes a computer to be unused.

By now, we should be thoroughly alarmed by AW. It is real, persistent, and certain to continue. But, what can we do about it? Truthfully, 100% protection is not possible. But we can lower our risk. The solution requires a "holistic", integrated strategy that includes some engineering, but is mostly doctrine, training, and deterrence.

The most important part of the solution is our need for a comprehensive training doctrine. We usually know who to call to fix garrison PC virus problems. But we have no doctrine in Electronic Warfare (EW) nor the simple, well known "Meaconing, Intrusion, Jamming, and Interference (MIJI) procedure that works in garrison or field.

With such a doctrine in place, Army-wide training efforts would be focused toward the best preventive effort. Of course, we may never completely stop soldiers from playing infected game software on government PCs, or buying pirated software in Itaewon Street in Korea and using it on government PCs. But training, awareness, and command support will induce greater caution and restraint, and this will reduce AW risks dramatically.

We also need a central AW agency, ideally at joint or national level. Another good model is the Joint Electronic Warfare Center (JEWC). At the very least, we need a central Army agency. This is not a new idea. A similar suggestion was made by a special DOD team in 1988, after the Internet Worm crisis.

Finally, we need legal tools for deterrence. Our UCMJ needs a specific article covering software piracy, hacking, computer sabotage, and knowingly making or introducing viruses. Such a UCMJ article could be formed under the authority of Title 10 USC 30. Coupled with understanding and awareness, deterrence would make the seriousness of the situation clearer. After all, even now there are individuals on the DDN MILNET who hack into other systems just to review or steal files, with impunity. Any good defense counsel would be amused watching a commander trying to fit the circumstances of modern intangible electronic "goods" theft to the elements of proof in our current UCMJ.

The big task will be building awareness and defenses at the DOD and national level--before it costs us our ability to sustain national level conflicts.

This will need our awareness and support. With luck and perseverance, we will be in time to build a good defense--before it costs us a blood price from a computer dependent soldier in battle.

Mr. Lewis, a former Signal Corps captain, is employed by LB&M Asscoiates, Inc. While on active duty, he was a Training Developer for Army Tactical Command & Control Systems (ATCCS) at TRADOC's integrating command, the Combined Arms Command for Training, Ft. Leavenworth, Kansas. He is a graduate of Eastern Kentucky University, Richmond, Kentucky, with a B.B.A. in Administrative Management and an A.S. in Graphic Technology. Other military assignments include Company Commander, Battalion S-1, DCSIM Radio Officer/Frequency Manager, and Signal Platoon Leader.