

~~SECRET~~

JUN 01 1995, NOFORN/INTL

pg 61+

Defense Intelligence Reference Document

May 1995

NGIC-1147-101-95

CIRC

Nonlethal Technologies—Worldwide (I)

REGRADED UNCLASSIFIED
ON MAY 28 1995
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-F

✓ NGIC COLLATERAL

100 156-617

100 156-617



~~SECRET~~

Contents

Foreword	xi
NONLETHAL CHEMICAL EFFECTORS WORLDWIDE	1
Introduction	1
Chemical Fuel Defeat Mechanisms	1
Gelation Agents	1
Combustion Modifiers	1
Additives for Air	2
Additives for Fuel	2
Weaponization/Countermeasures	2
Micrometal Oxidants	2
Overview	2
Former Soviet Union (FSU)	4
China	4
Capabilities	4
Acidification/Corrosion Agents	4
Overview	4
Foreign Interest	4
Abrasives	4
Foreign Interest	5
Sodium and Vanadium	5
Incapacitating Agents	5
Introduction	5
Riot-Control Agents (RCA)	5
Tear Agents	6
Vomiting Agents	7
Incapacitants	7
Psychochemicals	13
Paralyzants	13
Obscurants	14
Introduction	14
Neutral Obscurants	14
Agent Obscurants	17
Embrittling Compounds	18
Net Assessment	19
NONLETHAL BIOTECHNICAL EFFECTORS WORLDWIDE	23
Introduction	23
Fuel Stabilization Foams	25

REGRADED UNCLASSIFIED
ON ~~MAY 28 1987~~
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

Contents (Continued)

Former Soviet Union (FSU)	25
Biocorrosion Agents	25
Introduction	25
Former Soviet Union (FSU)	27
Net Assessment	27
NONLETHAL ACOUSTIC EFFECTORS WORLDWIDE	31
Introduction	31
Intelligence Overview	31
Infrasound Bioeffects	37
Infrasound Generation and Propagation	38
Net Assessment	41
NONLETHAL ELECTROMAGNETIC EFFECTORS WORLDWIDE	43
Introduction	43
Radiofrequency Weapons	43
Laser Weapons	46
The Former Soviet Union (FSU)	46
The United Kingdom	47
Armenia	47
France and Germany	47
China	48
Iraq	49
Israel	49
Jordan	49
Commercial Laser Weaponization	49
Strobe Light	49
Net Assessment	49
KINETIC NONLETHAL EFFECTORS WORLDWIDE	53
Introduction	53
Grenades	53
Bulk Dispersal Systems	56
Entanglement/Nets	56
Baton Cartridges	60
Net Assessment	60
NONLETHAL INFORMATION EFFECTORS WORLDWIDE	61
Introduction	61
Electronic Intrusion	61
Malicious Software	64
Net Assessment	66
CONCLUSION	67
Nonlethal Chemical Warfare	67
Nonlethal Biotechnical Warfare	67
Nonlethal Acoustic Warfare	67

Contents (Continued)

Nonlethal Electromagnetic Warfare	68
Nonlethal Kinetic Warfare	68
Nonlethal Information Warfare	68
Distribution List	DL-1

Appendix

A. List of Abbreviations and Acronyms	69
---	----

Tables

1. Countries Vice Interest and Capabilities in Nonlethal Technologies (Extant and Emerging)	iv
2. Selected Nonlethal Chemical Agent Designator and Agent Effectiveness ...	6
3. Lacrimatory Grenade Chemical Effectors—Worldwide	8
4. Agent Obscurants Vice Spectrum Vulnerability	16
5. Countries Engaged in Liquid-Metal Embrittlement	18
6. Critical Contributing Technologies Required to Produce Chemical Nonlethal Fuel-Defeating Agents	20
7. Projected Foreign Chemical Nonlethal Fuels Defeat Capabilities—2000 ...	21
8. Critical Contributing Technologies Required to Produce Biological Nonlethal Fuel-Defeating Agents	29
9. Projected Foreign Biological Nonlethal Fuels Defeat Capabilities—2000 ...	29
10. Radiofrequency Weapons Technology—Worldwide	51
11. Countries vs. Nonlethal Laser Capabilities	51
12. Worldwide Stun Grenades	54

Figures

1. Tank Engine Exhaust Valves After 12-Second Combustion Modifier Test	3
2. Russian Mobile Lidar	3
3. French MP7 Jet 56	11
4. United Kingdom No. 83 N201	12
5. Israel Antiterror Weapon Model 5	13
6. Fuel Eating/Filter Clogging Microbe	24
7. Russian Fuel Cell Foam Sample	26
8. Russian Ultrationalist 3 February 1994 Claim of Secret Acoustics Weapons	32
9. Directed Acoustic Weapon Concept	34
10. Directed Acoustic Countermeasure	35
11. Engagement Scenario	36
12. Acoustical Detonation Wave Generator	36

REGRADED UNCLASSIFIED
ON MAY 28 1997

BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R

ix

~~SECRET~~

Contents (Continued)

13. Rep-Rated Cruise Missile Concept	44
14. Russian High-Power Microwave Countermine System	45
15. Model of Russian 50 kW High Power Laser System	47
16. Schematic of Russian Gas-Dynamic Laser Mobile Complex for Remote Cutting	48
17. South African Strobe Light	50
18. French MR-35 Punch	57
19. French Water Cannon-Models VID 5,000, 8,000, and 12,000	58
20. Polish Antipersonnel Net System	59
21. Airborne Information Distortion	62
22. Advertisements for Virus, Norms, etc.	63
23. Remote Insertion of Malicious Software	65

NONLETHAL INFORMATION EFFECTORS WORLDWIDE

5 USC 552 (b) (1)

Introduction

(S/NF)

(U) Computer viruses are another unconventional disabling effect, already alarmingly demonstrated by hackers, both domestic and international. The information warfare technologies addressed in this section, i.e., computer viruses/malicious codes, information distortion, and surreptitious insertion loom as some of the greatest potential threats to a digitized, information-based modern army. Undetected, such weapons could disrupt tactical or even national defense mechanisms of a computer-dependent infrastructure.

(U) Increasing concentration of information in computers, computer systems, and networks that support command, control, communications, intelligence, and other military applications has made information technology a competitive weapon of unparalleled power and importance. At the same time, the utilization of information technology has made possible the compromise or corruption of critical information and the disruption of information services.

(U) Both electronic intrusion into computers and networks and the use of malicious software (computer viruses, Trojan horses, worms, logic bombs, and the like) have the capability to supply an adversary with the

data, modify and manipulate data, or disrupt operation of computer systems.

Electronic Intrusion

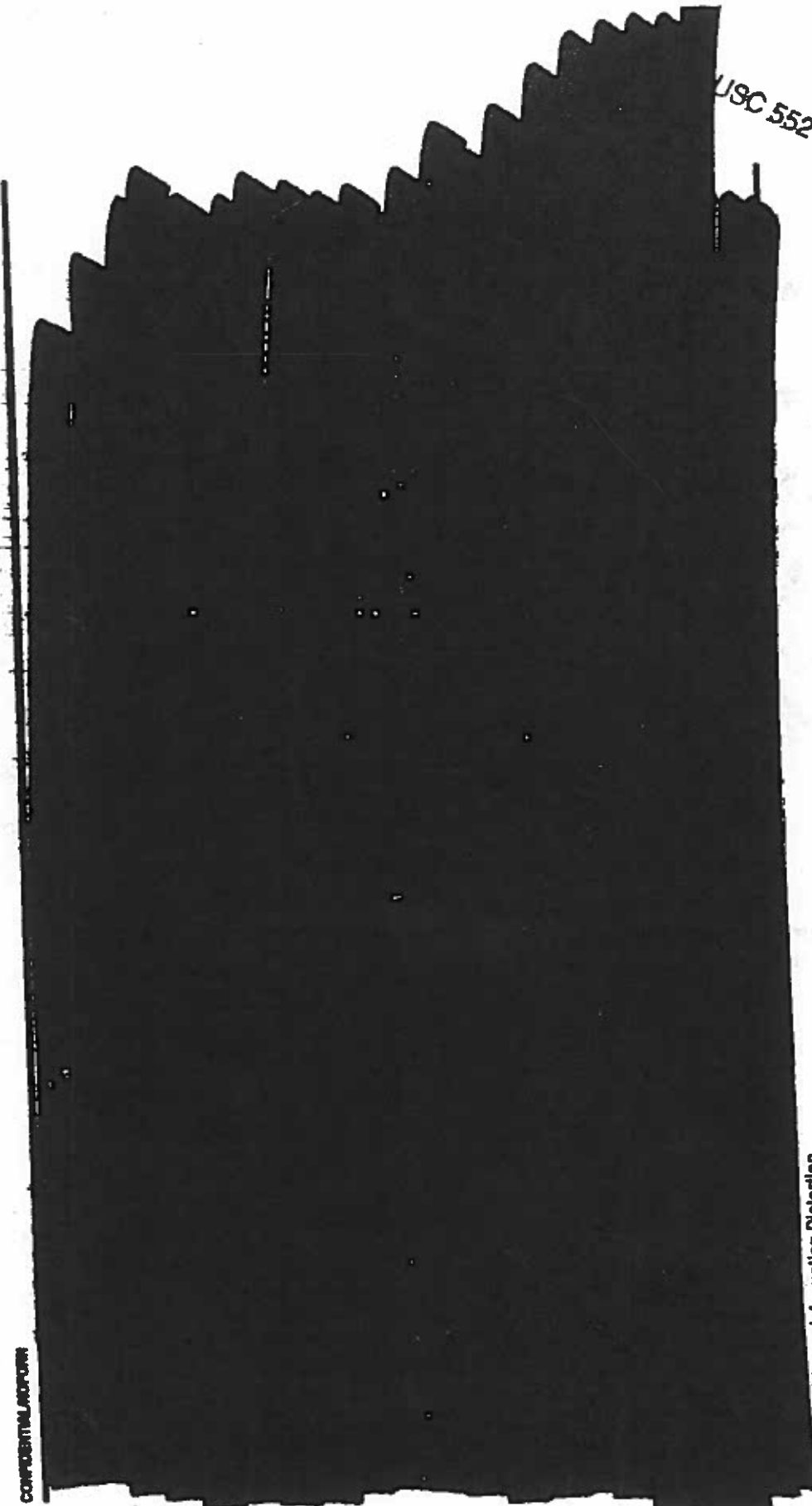
(U) Experts have assessed that computers with network connectivity or dial-up access can be entered by an electronic intruder from anywhere in the world. Gaining access to these computers through a network connection is relatively simple, costs very little, and typically involves little risk of detection. Information on systems and networks is readily available from a variety of sources, including professional journals, textbooks, and computer bulletin boards. Information about operating system vulnerabilities is frequently provided in publications of the computer underground. Many intruders are familiar with phone company equipment and software.

(U) In general, to access an automated information system, an intruder must obtain system user identification and passwords. These may be provided by legitimate users (intentionally or unintentionally), found by testing common or logical passwords, or through use of certain software tools. The intruder then attempts to identify and take advantage of known vulnerabilities in the hardware, software, or system operation. Once an intruder has gained access to a system of interest, he may install a trap door—a software mechanism that permits system protection to be circumvented and allows the intruder to reenter the system undetected.

(FOUO) Once an intruder obtains a valid password/ID, he can masquerade as a legitimate user. If the intruder can access the account of a system administrator or system programmer, he can grant himself "superuser" privileges allowing him to modify or delete

SECRET

NOFORN
USC 552 (b) (1)



CONFIDENTIAL/NOFORN

Figure 21. Airborne Information Distortion

SECRET

programs, data, index tables, and legitimate user privileges. In addition, he can then alter the audit trail to hide his presence. When inside the system, the intruder has the opportunity to modify data or programs.

(S/NF/WN) Intruders often share information through electronic bulletin boards (BBS), electronic computer magazines (ECM—sometimes called phracks), and other publications of the computer underground. BBS and ECM provide tips and techniques on computers, operating systems, passwords, computer addresses, hacking, data encryption and decryption, telephone systems, and manipulating the telephone system (phreaking). Similar information is frequently available in mainstream computer publications as well. One phrack even contained information on the data encryption standard (DES). DES, a complex nonlinear ciphering algorithm is one of the most frequently used encryption methods (figure 22).

(S/NF/WN) Defense and defense-related computers have been subject to intrusions of this type on a number of occasions:

- Over a period of several years (ending with their arrests in March 1989), a group of former West Germans now referred to as the "Hannover hackers" used telephone lines from Karlsruhe and Han-

nover to access over 250 computer systems. These included databases or networks hosted by at least 90 US defense or defense-related facilities.

- According to press reports, Dutch teenagers gained access, apparently through an INTERNET connection, to computer systems at 34 DoD sites (including the Air Force Weapons Laboratory, the David Taylor Research Center, the Army Information Systems Command, and the Navy Ocean Systems Center) during Operations Desert Shield/Storm. They were snooping in sensitive rather than classified military information. The intrusions normally involved broad-based keyword searches including such words as "rockets," "missiles," and "weapons." They exploited a trap door to permit future access and modified and copied military information to unauthorized accounts on US university systems. Although no "customer" was identified, the data collected by this group could have been sent electronically anywhere in the world.

UNCLASSIFIED

Information Available from Computer Magazines

The following advertisements were copied from the December 1991 issue of Computer Craft (formerly Modern Electronics).

COMPUTER PHREAKING

TROJAN HORSES, VIRUSES, WORMS, etc. and countermeasures. Includes disk with 250K+ of hacker text files and utilities, and legendary FLUSHOT+ protection system (ED. Choice, PC Magazine). Dozens of computer crime and abuse methods and countermeasures. How systems are penetrated. BBS advice, password defeats, glossary, much more! Manuals + Disks* \$39.

BEYOND VAN ECK PHREAKING

Eavesdropping on VDT and TV video signals using an ordinary TV! Ranges up to 1KM. Plans, countermeasures. Includes legal Van Eck uses, and original Top Secret Van Eck design! \$29.

CRYPTANALYSIS TECH.

Five powerful menu-driven crypto programs (in .COM and their .BAS sources) to analyze, decrypt "secure" ciphertexts. Worked-out examples. Recommended in prestigious COMPUTERS & SECURITY. Manual + Disk \$29.

Figure 22. Advertisements for Virus, Norma, etc.

SECRET

- An unauthorized user entered several systems at Lawrence Livermore National Laboratory in early December, 1988, using a vulnerability in the file transfer protocol of UNIX to achieve system manager status. This allowed him access to six Sun workstations and VAX machines. Although the intrusion was detected, officials are not sure what the hacker did because he removed and altered audit records. He did not appear to be after any particular information but seemed to be interested only in breaking into new systems. The hacker used the INTERNET and routed his calls through computers in several universities including Stanford, the University of Washington, and a research laboratory in New Jersey.

- In June 1992, British authorities arrested a group of hackers in the United Kingdom. Data retained by the hackers included information on computers in New Zealand, Belgium, Finland, and other countries; password files from various computers; and transcripts of "chat" sessions between themselves and other hackers. Although the full extent of their activities is still unclear, a review of information to date indicates that the hackers accessed the following computers:

552 (b) (1)

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

(S/NF) Electronic intrusion is a significant and growing threat. An intruder can obtain access to systems through network interconnectivity from virtually anywhere in the world because of the interconnection of the public telephone system and military and civil communication systems. The collective skill set of unauthorized users is high. The globalization of network connections and the availability of information about how to conduct attacks allows this skill set to be widely shared. In addition to providing an avenue for attack, network connectivity also provides a means by which attacks can be coordinated. Foreign Intelligence Ser-

vices (FIS) clearly are interested in the skills required to access automated information systems; they may be interested in the hackers themselves as well. While individuals operating independently represent primarily nuisance threats, the orchestration of groups of unauthorized users is potentially very serious.

Malicious Software

(U) Malicious software is software that is engineered to cause a computer to act in a manner other than that intended by its users and includes such programs as Trojan horses, logic bombs, worms, trap doors, bacteria, computer viruses, password traps, and others (figure 23). Examples include software designed to circumvent security systems, illicitly access data or processors, cause damage to computing systems or machinery controlled by them, modify or destroy data, or initiate processes or actions unintended by the computer operator. Malicious software can cause loss of productivity, system interference or lockup, corrupted files, loss of data, unreliable applications, or even system crashes. Eradicating the code can cost an organization hundreds of thousands of dollars, both in terms of lost data and the time it takes to recover from a malicious software attack. If the attack occurs during a critical military operation, the results could be deadly.

(U) Malicious software is already pervasive throughout the world and the capability for its production is growing. Although there have been no verified incidents of deliberate use of malicious software against the United States by an adversary, it could, and may in the future, be targeted against communications, transportation, banking, power, and computation systems upon which both industry and the military might depend. While viruses are far more prevalent than Trojan horses, worms, or logic bombs, the latter have the potential to do far greater damage. They are harder to detect and are generally written by more expert programmers with specific goals in mind.

(S) Many foreign countries have been the source of malicious software [REDACTED]. The country of origin, however, is not always apparent because, for

SECRET/NOFORN

(S-NF) [REDACTED]

(S-NF) [REDACTED]

Source [REDACTED]

Figure 23. Remote Insertion of Malicious Software

example, a computer virus can propagate through any number of computer systems before it is discovered. It is not surprising then that documented evidence of actual malicious code introduction by FIS or military is not available. An adversary would not be willing to expose such a capability during peacetime. There has been evidence of FIS intent to introduce computer viruses, however.

~~(S/NF/NOINTEL)~~ Prior to the August 1991 coup attempt, the KGB was developing computer viruses with the intent of using them to disrupt computer systems during times of war or crisis. In early 1991, a highly restricted project was undertaken by a group within the Military Intelligence Directorate of Cuba's Ministry of the Armed Forces. The group was instructed to obtain information to develop a computer virus to infect US civilian computers. The group spent about \$5,000 to buy open-source data on computer networks, computer

viruses, SATCOM, and related communications technology. Details of this specific endeavor are not known, however, the point is that such efforts continue to be made and could potentially cause irreparable harm to any nations' defense.

~~(C)~~ The scope for the military use of malicious software, both strategically and tactically, is large, and as the offensive potential for this type of weapon becomes apparent, governments are more likely to become involved in malicious software research [REDACTED]

~~(S)~~ In addition to military targets, adversaries may target a country's infrastructure as well—public

SECRET 552 (b) (1)



telecommunications, financial networks, power grids, transportation (air traffic control systems)—systems upon which government, industry, and military depend. Similarly, the adversaries may not be military or government groups but terrorist organizations, political/social activists, or commercial entities. No such groups have been specifically identified as having an interest in the use of malicious software or assessed to have the capability to use it. There are any number of permutations of motives, means, and targets that can be attributed to such groups, and because little is known about them, capabilities and intents are almost impossible to assess.

Net Assessment

(U) In addition to the information distortion possibilities of electronic transmissions to tactical systems, many other aspects of military command, control, communications, and intelligence (C3I) is controlled or influenced by computers. The reliance on computers, automated weapons, and other automated systems critical to the performance of military missions has grown tremendously in recent years and will continue unabated into the next century. Computer viruses and other malicious software are already pervasive throughout the world, and the capability for its production is growing. Probably every country in the world where there is a computer has been victimized at least once by malicious software, and more than 60 different countries have been identified as the source of at least one computer virus.

(S/AF) The development of malicious software requires little in the way of resources—a few computers and an individual or group with the appropriate expertise—making a malicious software R&D program easy to support as well as easy to hide. Inserting the malicious software into the target system, however, is more problematic. Trusted insiders may have to be recruited or electronic intrusion methods attempted.



5 USC 552 (b) (1)



National Security Archive,
Suite 701, Gelman Library, The George Washington University,
2130 H Street, NW, Washington, D.C., 20037,
Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu