The US Army War College Quarterly: Parameters

Volume 28
Number 1 *Parameters Spring 1998*

Article 12

2-17-1998

The Mind Has No Firewall

Timothy L. Thomas

The Mind Has No Firewall

TIMOTHY L. THOMAS

From *Parameters*, Spring 1998, pp. 84-92.

> "It is completely clear that the state which is first to create such weapons will achieve incomparable superiority." -- Major I. Chernishev, Russian army[1]

The human body, much like a computer, contains myriad data processors. They include, but are not limited to, the chemical-electrical activity of the brain, heart, and peripheral nervous system, the signals sent from the cortex region of the brain to other parts of our body, the tiny hair cells in the inner ear that process auditory signals, and the light-sensitive retina and cornea of the eye that process visual activity.[2] We are on the threshold of an era in which these data processors of the human body may be manipulated or debilitated. Examples of unplanned attacks on the body's data-processing capability are well-documented. Strobe lights have been known to cause epileptic seizures. Not long ago in Japan, children watching television cartoons were subjected to pulsating lights that caused seizures in some and made others very sick.

Defending friendly and targeting adversary data-processing capabilities of the body appears to be an area of weakness in the US approach to information warfare theory, a theory oriented heavily toward systems data-processing and designed to attain information dominance on the battlefield. Or so it would appear from information in the open, unclassified press. This US shortcoming may be a serious one, since the capabilities to alter the data- processing systems of the body already exist. A recent edition of *U.S. News and World Report* highlighted several of these "wonder weapons" (acoustics, microwaves, lasers) and noted that scientists are "searching the electromagnetic and sonic spectrums for wavelengths that can affect human behavior."[3] A recent Russian military article offered a slightly different slant to the problem, declaring that "humanity stands on the brink of a psychotronic war" with the mind and body as the focus. That article discussed Russian and international attempts to control the psycho-physical condition of man and his decisionmaking processes by the use of VHF-generators, "noiseless cassettes," and other technologies.

An entirely new arsenal of weapons, based on devices designed to introduce subliminal messages or to alter the body's psychological and data-processing capabilities, might be used to incapacitate individuals. These weapons aim to control or alter the psyche, or to attack the various sensory and data-processing systems of the human organism. In both cases, the goal is to confuse or destroy the signals that normally keep the body in equilibrium.

This article examines energy-based weapons, psychotronic weapons, and other developments designed to alter the ability of the human body to process stimuli. One consequence of this assessment is that the way we commonly use the term "information warfare" falls short when the individual soldier, not his equipment, becomes the target of attack.

Information Warfare Theory and the Data-Processing Element of Humans

In the United States the common conception of information warfare focuses primarily on the capabilities of hardware systems such as computers, satellites, and military equipment which process data in its various forms. According to Department of Defense Directive S-3600.1 of 9 December 1996, information warfare is defined as "an information operation conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries." An information operation is defined in the same directive as "actions taken to affect adversary information and information systems while defending one's own information and information systems." These "information systems" lie at the heart of the modernization effort of the US armed forces and other countries, and manifest themselves as hardware, software, communications capabilities, and highly trained individuals. Recently, the

US Army conducted a mock battle that tested these systems under simulated combat conditions.

US Army Field Manual 101-5-1, *Operational Terms and Graphics* (released 30 September 1997), defines information warfare as "actions taken to achieve information superiority by affecting a hostile's information, information based-processes, and information systems, while defending one's own information, information processes, and information systems." The same manual defines information operations as a "continuous military operation within the military information environment that enables, enhances, and protects friendly forces' ability to collect, process, and act on information to achieve an advantage across the full range of military operations. [Information operations include] interacting with the Global Information Environment . . . and exploiting or denying an adversary's information and decision capabilities."[4]

This "systems" approach to the study of information warfare emphasizes the use of data, referred to as information, to penetrate an adversary's physical defenses that protect data (information) in order to obtain operational or strategic advantage. It has tended to ignore the role of the human body as an information- or data-processor in this quest for dominance except in those cases where an individual's logic or rational thought may be upset via disinformation or deception. As a consequence little attention is directed toward protecting the mind and body with a firewall as we have done with hardware systems. Nor have any techniques for doing so been prescribed. Yet the body is capable not only of being deceived, manipulated, or misinformed but also shut down or destroyed--just as any other data-processing system. The "data" the body receives from external sources--such as electromagnetic, vortex, or acoustic energy waves--or creates through its own electrical or chemical stimuli can be manipulated or changed just as the data (information) in any hardware system can be altered.

The only body-related information warfare element considered by the United States is psychological operations (PSYOP). In Joint Publication 3-13.1, for example, PSYOP is listed as one of the elements of command and control warfare. The publication notes that "the ultimate target of [information warfare] is the information dependent process, whether human or automated . . . . Command and control warfare (C2W) is an application of information warfare in military operations. . . . C2W is the integrated use of PSYOP, military deception, operations security, electronic warfare and physical destruction."[5]

One source defines information as a "nonaccidental signal used as an input to a computer or communications system."[6] The human body is a complex communication system constantly receiving nonaccidental and accidental signal inputs, both external and internal. If the ultimate target of information warfare is the information-dependent process, "whether human or automated," then the definition in the joint publication implies that human data-processing of internal and external signals can clearly be considered an aspect of information warfare. Foreign researchers have noted the link between humans as data processors and the conduct of information warfare. While some study only the PSYOP link, others go beyond it. As an example of the former, one recent Russian article described offensive information warfare as designed to "use the Internet channels for the purpose of organizing PSYOP as well as for `early political warning' of threats to American interests."[7] The author's assertion was based on the fact that "all mass media are used for PSYOP . . . [and] today this must include the Internet." The author asserted that the Pentagon wanted to use the Internet to "reinforce psychological influences" during special operations conducted outside of US borders to enlist sympathizers, who would accomplish many of the tasks previously entrusted to special units of the US armed forces.

Others, however, look beyond simple PSYOP ties to consider other aspects of the body's data-processing capability. One of the principal open source researchers on the relationship of information warfare to the body's data-processing capability is Russian Dr. Victor Solntsev of the Baumann Technical Institute in Moscow. Solntsev is a young, well-intentioned researcher striving to point out to the world the potential dangers of the computer operator interface. Supported by a network of institutes and academies, Solntsev has produced some interesting concepts.[8] He insists that man must be viewed as an open system instead of simply as an organism or closed system. As an open system, man communicates with his environment through information flows and communications media. One's physical environment, whether through electromagnetic, gravitational, acoustic, or other effects, can cause a change in the psycho-physiological condition of an organism, in Solntsev's opinion. Change of this sort could directly affect the mental state and consciousness of a computer operator. This would not be electronic war or information warfare in the traditional sense, but rather in a nontraditional and non-US sense. It might encompass, for example, a computer

modified to become a weapon by using its energy output to emit acoustics that debilitate the operator. It also might encompass, as indicated below, futuristic weapons aimed against man's "open system."

Solntsev also examined the problem of "information noise," which creates a dense shield between a person and external reality. This noise may manifest itself in the form of signals, messages, images, or other items of information. The main target of this noise would be the consciousness of a person or a group of people. Behavior modification could be one objective of information noise; another could be to upset an individual's mental capacity to such an extent as to prevent reaction to any stimulus. Solntsev concludes that all levels of a person's psyche (subconscious, conscious, and "superconscious") are potential targets for destabilization.

According to Solntsev, one computer virus capable of affecting a person's psyche is Russian Virus 666. It manifests itself in every 25th frame of a visual display, where it produces a combination of colors that allegedly put computer operators into a trance. The subconscious perception of the new pattern eventually results in arrhythmia of the heart. Other Russian computer specialists, not just Solntsev, talk openly about this "25th frame effect" and its ability to subtly manage a computer user's perceptions. The purpose of this technique is to inject a thought into the viewer's subconscious. It may remind some of the subliminal advertising controversy in the United States in the late 1950s.

US Views on "Wonder Weapons": Altering the Data-Processing Ability of the Body

What technologies have been examined by the United States that possess the potential to disrupt the data-processing capabilities of the human organism? The 7 July 1997 issue of *U.S. News and World Report* described several of them designed, among other things, to vibrate the insides of humans, stun or nauseate them, put them to sleep, heat them up, or knock them down with a shock wave.[9] The technologies include dazzling lasers that can force the pupils to close; acoustic or sonic frequencies that cause the hair cells in the inner ear to vibrate and cause motion sickness, vertigo, and nausea, or frequencies that resonate the internal organs causing pain and spasms; and shock waves with the potential to knock down humans or airplanes and which can be mixed with pepper spray or chemicals.[10]

With modification, these technological applications can have many uses. Acoustic weapons, for example, could be adapted for use as acoustic rifles or as acoustic fields that, once established, might protect facilities, assist in hostage rescues, control riots, or clear paths for convoys. These waves, which can penetrate buildings, offer a host of opportunities for military and law enforcement officials. Microwave weapons, by stimulating the peripheral nervous system, can heat up the body, induce epileptic-like seizures, or cause cardiac arrest. Low-frequency radiation affects the electrical activity of the brain and can cause flu-like symptoms and nausea. Other projects sought to induce or prevent sleep, or to affect the signal from the motor cortex portion of the brain, overriding voluntary muscle movements. The latter are referred to as pulse wave weapons, and the Russian government has reportedly bought over 100,000 copies of the "Black Widow" version of them.[11]

However, this view of "wonder weapons" was contested by someone who should understand them. Brigadier General Larry Dodgen, Deputy Assistant to the Secretary of Defense for Policy and Missions, wrote a letter to the editor about the "numerous inaccuracies" in the *U.S. News and World Report* article that "misrepresent the Department of Defense's views."[12] Dodgen's primary complaint seemed to have been that the magazine misrepresented the use of these technologies and their value to the armed forces. He also underscored the US intent to work within the scope of any international treaty concerning their application, as well as plans to abandon (or at least redesign) any weapon for which countermeasures are known. One is left with the feeling, however, that research in this area is intense. A concern not mentioned by Dodgen is that other countries or non-state actors may not be bound by the same constraints. It is hard to imagine someone with a greater desire than terrorists to get their hands on these technologies. "Psycho-terrorism" could be the next buzzword.

Russian Views on "Psychotronic War"

The term "psycho-terrorism" was coined by Russian writer N. Anisimov of the Moscow Anti-Psychotronic Center. According to Anisimov, psychotronic weapons are those that act to "take away a part of the information which is stored in a man's brain. It is sent to a computer, which reworks it to the level needed for those who need to control the man, and the modified information is then reinserted into the brain." These weapons are used against the mind to induce hallucinations, sickness, mutations in human cells, "zombification," or even death. Included in the arsenal are

VHF generators, X-rays, ultrasound, and radio waves. Russian army Major I. Chernishev, writing in the military journal *Orienteer* in February 1997, asserted that "psy" weapons are under development all over the globe. Specific types of weapons noted by Chernishev (not all of which have prototypes) were:

- A psychotronic generator, which produces a powerful electromagnetic emanation capable of being sent through telephone lines, TV, radio networks, supply pipes, and incandescent lamps.
- An autonomous generator, a device that operates in the 10-150 Hertz band, which at the 10-20 Hertz band forms an infrasonic oscillation that is destructive to all living creatures.
- A nervous system generator, designed to paralyze the central nervous systems of insects, which could have the same applicability to humans.
- Ultrasound emanations, which one institute claims to have developed. Devices using ultrasound emanations are supposedly capable of carrying out bloodless internal operations without leaving a mark on the skin. They can also, according to Chernishev, be used to kill.
- Noiseless cassettes. Chernishev claims that the Japanese have developed the ability to place infra-low frequency voice patterns over music, patterns that are detected by the subconscious. Russians claim to be using similar "bombardments" with computer programming to treat alcoholism or smoking.
- The 25th-frame effect, alluded to above, a technique wherein each 25th frame of a movie reel or film footage contains a message that is picked up by the subconscious. This technique, if it works, could possibly be used to curb smoking and alcoholism, but it has wider, more sinister applications if used on a TV audience or a computer operator.
- Psychotropics, defined as medical preparations used to induce a trance, euphoria, or depression. Referred to as "slow-acting mines," they could be slipped into the food of a politician or into the water supply of an entire city. Symptoms include headaches, noises, voices or commands in the brain, dizziness, pain in the abdominal cavities, cardiac arrhythmia, or even the destruction of the cardiovascular system.

There is confirmation from US researchers that this type of study is going on. Dr. Janet Morris, coauthor of *The Warrior's Edge*, reportedly went to the Moscow Institute of Psychocorrelations in 1991. There she was shown a technique pioneered by the Russian Department of Psycho-Correction at Moscow Medical Academy in which researchers electronically analyze the human mind in order to influence it. They input subliminal command messages, using key words transmitted in "white noise" or music. Using an infra-sound, very low frequency transmission, the acoustic psycho-correction message is transmitted via bone conduction.[13]

In summary, Chernishev noted that some of the militarily significant aspects of the "psy" weaponry deserve closer research, including the following nontraditional methods for disrupting the psyche of an individual:

- ESP research: determining the properties and condition of objects without ever making contact with them and "reading" peoples' thoughts
- Clairvoyance research: observing objects that are located just beyond the world of the visible--used for intelligence purposes
- Telepathy research: transmitting thoughts over a distance--used for covert operations
- Telekinesis research: actions involving the manipulation of physical objects using thought power, causing them to move or break apart--used against command and control systems, or to disrupt the functioning of weapons of mass destruction
- Psychokinesis research: interfering with the thoughts of individuals, on either the strategic or tactical level

While many US scientists undoubtedly question this research, it receives strong support in Moscow. The point to underscore is that individuals in Russia (and other countries as well) believe these means can be used to attack or steal from the data-processing unit of the human body.

Solntsev's research, mentioned above, differs slightly from that of Chernishev. For example, Solntsev is more interested in hardware capabilities, specifically the study of the information-energy source associated with the computer-operator interface. He stresses that if these energy sources can be captured and integrated into the modern computer, the result will be a network worth more than "a simple sum of its components." Other researchers are studying high-frequency generators (those designed to stun the psyche with high frequency waves such as

electromagnetic, acoustic, and gravitational); the manipulation or reconstruction of someone's thinking through planned measures such as reflexive control processes; the use of psychotronics, parapsychology, bioenergy, bio fields, and psychoenergy;[14] and unspecified "special operations" or anti-ESP training.

The last item is of particular interest. According to a Russian TV broadcast, the strategic rocket forces have begun anti-ESP training to ensure that no outside force can take over command and control functions of the force. That is, they are trying to construct a firewall around the heads of the operators.

Conclusions

At the end of July 1997, planners for Joint Warrior Interoperability Demonstration '97 "focused on technologies that enhance real-time collaborative planning in a multinational task force of the type used in Bosnia and in Operation Desert Storm. The JWID '97 network, called the Coalition Wide-Area Network (CWAN), is the first military network that allows allied nations to participate as full and equal partners."[15] The demonstration in effect was a trade fair for private companies to demonstrate their goods; defense ministries got to decide where and how to spend their money wiser, in many cases without incurring the cost of prototypes. It is a good example of doing business better with less. Technologies demonstrated included:[16]

- Soldiers using laptop computers to drag cross-hairs over maps to call in airstrikes
- Soldiers carrying beepers and mobile phones rather than guns
- Generals tracking movements of every unit, counting the precise number of shells fired around the globe, and inspecting real-time damage inflicted on an enemy, all with multicolored graphics[17]

Every account of this exercise emphasized the ability of systems to process data and provide information feedback via the power invested in their microprocessors. The ability to affect or defend the data-processing capability of the human operators of these systems was never mentioned during the exercise; it has received only slight attention during countless exercises over the past several years. The time has come to ask why we appear to be ignoring the operators of our systems. Clearly the information operator, exposed before a vast array of potentially immobilizing weapons, is the weak spot in any nation's military assets. There are few international agreements protecting the individual soldier, and these rely on the good will of the combatants. Some nations, and terrorists of every stripe, don't care about such agreements.

This article has used the term data-processing to demonstrate its importance to ascertaining what so-called information warfare and information operations are all about. Data-processing is the action this nation and others need to protect. Information is nothing more than the output of this activity. As a result, the emphasis on information-related warfare terminology ("information dominance," "information carousel") that has proliferated for a decade does not seem to fit the situation before us. In some cases the battle to affect or protect data-processing elements pits one mechanical system against another. In other cases, mechanical systems may be confronted by the human organism, or vice versa, since humans can usually shut down any mechanical system with the flip of a switch. In reality, the game is about protecting or affecting signals, waves, and impulses that can influence the data-processing elements of systems, computers, or people. We are potentially the biggest victims of information warfare, because we have neglected to protect ourselves.

Our obsession with a "system of systems," "information dominance," and other such terminology is most likely a leading cause of our neglect of the human factor in our theories of information warfare. It is time to change our terminology and our conceptual paradigm. Our terminology is confusing us and sending us in directions that deal primarily with the hardware, software, and communications components of the data-processing spectrum. We need to spend more time researching how to protect the humans in our data management structures. Nothing in those structures can be sustained if our operators have been debilitated by potential adversaries or terrorists who--right now--may be designing the means to disrupt the human component of our carefully constructed notion of a system of systems.

NOTES

1. I. Chernishev, "Can Rulers Make `Zombies' and Control the World?" *Orienteer*, February 1997, pp. 58-62.

2. Douglas Pasternak, "Wonder Weapons," *U.S. News and World Report*, 7 July 1997, pp. 38-46.

3. Ibid., p. 38.

4. FM 101-5-1, *Operational Terms and Graphics*, 30 September 1997, p. 1-82.

5. Joint Pub 3-13.1, *Joint Doctrine for Command and Control Warfare (C2W)*, 7 February 1996, p. v.

6. The American Heritage Dictionary (2d College Ed.; Boston: Houghton Mifflin, 1982), p. 660, definition 4.

7. Denis Snezhnyy, "Cybernetic Battlefield & National Security," *Nezavisimoye Voyennoye Obozreniye*, No. 10, 15-21 March 1997, p. 2.

8. Victor I. Solntsev, "Information War and Some Aspects of a Computer Operator's Defense," talk given at an Infowar Conference in Washington, D.C., September 1996, sponsored by the National Computer Security Association. Information in this section is based on notes from Dr. Solntsev's talk.

9. Pasternak, p. 40.

10. Ibid., pp. 40-46.

11. Ibid.

12. Larry Dodgen, "Nonlethal Weapons," *U.S. News and World Report*, 4 August 1997, p. 5.

13. "Background on the Aviary," Nexus Magazine, downloaded from the Internet on 13 July 1997 from www.execpc.com/vjentpr/nexusavi.html, p.7.

14. Aleksandr Cherkasov, "The Front Where Shots Aren't Fired," *Orienteer*, May 1995, p. 45. This article was based on information in the foreign and Russian press, according to the author, making it impossible to pinpoint what his source was for this reference.

15. Bob Brewin, "DOD looks for IT `golden nuggets,'" *Federal Computer Week*, 28 July 1997, p. 31, as taken from the Earlybird Supplement, 4 August 1997, p. B 17.

16. Oliver August, "Zap! Hard day at the office for NATO's laptop warriors," *The Times*, 28 July 1997, as taken from the Earlybird Supplement, 4 August 1997, p. B 16.

17. Ibid.

Lieutenant Colonel Timothy L. Thomas (USA Ret.) is an analyst at the Foreign Military Studies Office, Fort Leavenworth, Kansas. Recently he has written extensively on the Russian view of information operations and on current Russian military-political issues. During his military career he served in the 82d Airborne Division and was the Department Head of Soviet Military-Political Affairs at the US Army's Russian Institute in Garmisch, Germany.

Reviewed 25 February 1998. Please send comments or corrections to carl_Parameters@conus.army.mil