Reprinted courtesy of the Strategic Studies Institute
United States Army War College, Carlisle Barracks, PA

Metaphors and Modern Threats: Biological, Computer, and Cognitive Viruses

By

Edmund M. Glabus
Aegis Research Corporation
7799 Leesburg Pike, Suite 1100 North
Falls Church, VA 22043
March 31, 1998

Introduction

One challenge of national security planning and force protection programming is how to visualize military threats. For current operations, this task is made difficult by the sheer volume of information we receive purporting to help us understand threats to military and civilian assets and operations. Unfortunately, military decision-makers, planners, and analysts are often exposed to more information about any given situation than they can assimilate within normal operational and time constraints. When planning for future strategies and capabilities, the converse is true. Instead of too much information, we suffer from too little. Analysts, planners, and leaders understandably are hesitant to "bet the farm" on predictions, projections, or forecasts about future adversaries and scenarios.

However, time and events wait for no man. In the short term the budget calendar, Program Objective Memorandum (POM) timeline, and systems acquisition and fielding cycles all drive Department of Defense personnel to identify assumptions, derive conclusions, present recommendations, and make decisions. The military leadership's emphasis on extending our conceptual horizons (e.g., *Joint Vision 2010*, *Army 2010*, the Army After Next Project, etc.) also impels us to complete similar actions with even less clarity and confidence in our assessments. As a result many decision-makers, planners, and analysts use only a few, highly representative pieces of information to reduce problems to a manageable size.

In the extraordinary, complicated environment of military strategy, decision-makers and staffs will use these shortcuts, or heuristics, to classify situations according to a few key features and guide their thinking (and learning). There is nothing inherently wrong with this shortcut

98

approach to planning and decision making, as long as our heuristics are reasonably representative. One favorite technique is the use of the metaphor. As Martin Libicki writes:

> Used properly, a metaphor can be a starting point for analysis, a littoral, as it were, between the land of the known and the ocean of the unfamiliar. A good metaphor can help frame the questions that might otherwise not arise, it can illustrate relationships whose importance might otherwise be overlooked, and it can provide a useful heuristic device, a way to play with concepts, to hold them up to the light to catch the right reflections, and to tease out questions for further inquiry.[1]

One useful metaphor we can use to visualize modern threats is that of the virus. Most of us have some degree familiarity with viruses, either through a personal period of sickness, family member illness, or perhaps from biology and health classes in school. Usually we are aware of related terms like vaccine, inoculation, and antibiotic. Viruses are mysterious creatures to some, but reference to virus threats has achieved a degree of acceptance in national security discussions. Two developments contributing to this acceptance are the recent emphasis on information warfare/information operations, with a strong focus on computers, and an unfortunate resurgence in biological warfare activities on both the international and domestic scenes.

Before we can discuss using viruses as a threat metaphor, however, we need to define the term in a conventional sense[2]:

vi-rus...[L, slimy liquid, poison, stench....]

1 archaic: venom emitted by a poisonous animal

2a : the causative agent of an infectious disease : disease germ

2b : FILTERABLE VIRUS; specifically : any of a large group of submicroscopic infective agents that are held by some to be living organisms and by others to be complex autocatalytic protein molecules containing nucleic acids and comparable to genes, that are capable of growth and multiplication only in living cells, and that cause various important diseases in man, animals, or plants....

2c : VIRUS DISEASE....

3 : a morbid corrupting quality in intellectual or moral conditions : something that poisons the mind or soul....

4 : an antigenic but not infective material (as vaccine lymph)....

In light of this formal definition, we will use this paper to explore the use of the virus as a metaphor to discuss threats that are difficult to visualize. We will focus on three threats that are subsets of biological warfare, computer network attack, and memetic warfare (Figure 1, shaded

---

[1] Martin C. Libicki, *Defending Cyberspace and Other Metaphors* (Washington, D.C.: Institute for National Strategic Studies/GPO, 1997), p. 6.

[2] *Webster's Third International Dictionary of the English Language, Unabridged* (Springfield, Mass.: Merriam-Webster, 1961), p. 2556.

area). Using the Army After Next Project's construct of doctrine/concept/idea[3], we can view the three types of warfare listed above through the metaphor of the virus, in order to present them in an easily understandable way. As we move from biological warfare, to computer network attack, to memetic warfare, out illustrations will cross the spectrum from doctrine, to concept, to idea.

Summary and Relationship of Virus Metaphors

In his book *Virus of the Mind: The New Science of the Meme*, Richard Brodie relies on metaphor to discuss what he concludes is a new form of virus. According to Richard Brodie, "viruses occur in three different universes: biology, computers, and the mind" (or cognition). The following table, adapted from one found in *Virus of the Mind*, "shows the correspondence between words used to talk about evolution and viruses in each of the three universes."[4] In this paper we will use Brodie's taxonomy to explore the use of the virus metaphor, and examine in turn the use of biological, computer, and cognitive viruses as threat metaphors.

Biology	Computers	Cognition
Gene	Machine Instruction	Meme
Cell	Computer [and Paper]	Mind
DNA	Machine Language	Brain Representations
Virus	Computer Virus	Virus of the Mind
Gene Pool	All Software	Meme Pool
Spores/Germs	Elect. Bulletin Board Postings	Broadcasts/Publications
Species	Operating System	Cultural Institutions
Genus/Higher Classifications	Machine Architecture	Culture
Organism	Program	Behavior/Artifact
Genetic Susceptibility	"Back Door" or Security Hole	Psychological Susceptibility or "Button"
Genetic Evolution	Artificial Life	Cultural Evolution

Biological Viruses: Definition and Threat Context

Firmly grounded in doctrine, biological warfare is "Employment of biological agents to produce casualties in man or animals and damage to plants or materiel; or defense against such employment[5]. It is the easiest type of warfare to discuss using the term virus, as viruses literally are part of the discipline. For purposes of this paper, we will use part 2b of the formal virus definition above to describe viruses when the term is associated with the biological threat. Although most closely related to the virus metaphor, biological warfare threats include more than viruses (e.g., bioregulators, bacteria, fungal toxins, and vectors). From a layman's perspective, though, these biological warfare threats can all be visualized in terms of viruses.

---

[3] *The Annual Report on the Army After Next Project to the Chief of Staff of the Army*, July 1997.
[4] Richard Brodie, *Virus of the Mind The New Science of the Meme* (Seattle: Integral Press, 1996), p. 56.
[5] *Joint Publication 1-02, Dictionary of Military and Associated Terms* (Washington, D.C.: GPO, 1989), p. 52. The definition of biological warfare actually says "See Biological Operation," an interesting parallel to current discussions about the relationship between information *warfare* and information *operations*.

100

As with most national security threats, the majority of official government analyses and estimates are classified. However, one particularly good open source document on the biological virus threat is the Office of the Secretary of Defense's *Proliferation: Threat and Response.*[6] In a concise threat statement, the OSD report concludes: "Biological weapons have the greatest potential for lethality of any weapon. Biological weapons are accessible to all countries; there are few barriers to developing such weapons with a modest level of effort. The current level of sophistication for many biological agents is low but there is enormous potential—based on advances in modern molecular biology, fermentation, and drug delivery technology—for making more sophisticated weapons."[7]

The magnitude of the biological warfare threat is difficult to convey, but one example gives an idea of the potential scope of the problem. According to an article by R. Jeffrey Smith, Washington post Staff Writer, Iraq has *declared* it maintained biological weapons including anthrax, botulinum toxin, aflatoxin, ricin, and gas gangrene. Let's use only the first two of these agents as examples.

- **Anthrax:** "This often fatal bacteria causes high fever, difficulty in breathing, chest pain and eventually blood poisoning. Antibiotics often prove useless after a short period. [Iraq has declared] 2,245 gallons, enough to kill billions. The U.N. suspects production was three to four times that."

- **Botulinum Toxin:** "This bacteria first causes vomiting, constipation, thirst, weakness, fever, dizziness, blurred vision, pupil dilation and difficulty in swallowing. Eventually it causes paralysis, respiratory failure, and often death. [Iraq has declared] 5,125 gallons, enough to wipe out Earth's population several times. The U.N. suspects the number may have been twice that."[8]

Although it is convenient to focus on one country, Iraq is not alone in this respect. The OSD report addresses potential research, production, testing, or weaponization of biological weapons by Iraq, North Korea, China, Iran, and Russia, among others.

Potential non-state actors include both foreign terrorist organizations and domestic groups. Recently in the U.S. a "microbiologist on probation for fraudulently obtaining bubonic plague toxins in Ohio in 1995, and...a Las Vegas area entrepreneur and home-laboratory medical researcher, were arrested...[and] charged with possessing anthrax for use as a weapon."[9] Although the vials contained a harmless anthrax strain for use in inoculating farm animals, FBI agents continued to investigate the potential for criminal wrongdoing. Other examples are more clear-cut. As Charles Mercier writes,

---

[6] Office of the Secretary of Defense, *Proliferation: Threat and Response* (Washington, D.C.: GPO, November 1997).
[7] *Proliferation: Threat and Response*, p. 81.
[8] R. Jeffrey Smith, "Poison, Germ Weapons Would Not Be Direct Targets," *The Washington Post,* February 22, 1998, p. A28. As a point of comparison, the average backyard pool has 25,000 gallons of water (Source: Customer service representative, Maryland Pools, Inc., Columbia, MD).
[9] William Claiborne, "Vials Seized by FBI in Las Vegas Are Found to Contain 'Harmless' Anthrax Vaccine," *The Washington Post*, February 22, 1998, p. A6.

> biological...agents can readily be developed by terrorists...[requiring] a college-level knowledge of biology or chemistry, less than $20,000 in supplies, and the forged documents or accomplices needed to obtain "seed" bacteria or precursor chemicals....a US neo-Nazi group (the Order of the Rising sun) produced 80 pounds of typhoid bacillus in 1972, and in 1984 Paris police raided an apartment rented by the Baader Meinhof gang and found flasks of Clostridium botulinum culture. More recently, Japanese police found 160 barrels of peptone (a growth media for bacteria) along with Clostridium botulinum when they raided an Aum Shinrikyo compound near Mount Fuji. Tricoecene mycotoxins (e.g., "yellow rain") can be produced simply using a corn meal slurry and the appropriate strain of fungus.[10]

In discussions of biological warfare, we can start by examining viruses in a literal sense, as part of the family of biological agents. It is very easy for us to then turn to other biological threats (e.g., bioregulators, bacteria, fungal toxins, and vectors) and apply the virus metaphor. However, a more interesting test is to apply the metaphor to information warfare, specifically the realms of computers and memetics.

Computer Viruses: Definition and Threat Context

With regard to joint doctrine, Computer Network Attack started out as an innovative idea, is currently undergoing refinement as a concept, and appears to be making a formal transition to doctrine. Computer network attack is currently defined as "operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves."[11] It was inserted in the draft of *Joint Publication 3-13, Information Operations*, and has survived the early rounds of staffing. Although computer network attack is not focused solely on defending against viruses ("hacking" without inserting viruses is a constant concern among military information security professionals), computer viruses are certainly a leading threat concern. The US Army's *Field Manual 100-6, Information Operations* also refers to virus threats, but the treatment is brief: "It is even possible that a military system could come from the factory with an embedded logic bomb or virus. In the past, new commercial floppy disks used by government agencies have been found to contain a virus upon delivery from the factory."[12]

We define computer viruses using Dr. Fred Cohen's *informal* definition. For our purposes, "a computer virus is a computer program that can infect other computer programs by modifying them in such a way as to include a (possibly evolved) copy of itself."[13] It is useful to

---

[10] Charles L. Mercier, Jr., "Terrorists, WMD, and the US Army Reserve, *Parameters*, Vol. 28, No. 3, Autumn 1997, pp. 101-102.

[11] Joint Pub 3-13pc, *Joint Doctrine for Information Operations, Preliminary Coordination*, 28 Jan 98, Glossary.

[12] Army Field Manual 100-6, *Information Operations* (Washington, DC: Department of the Army/GPO, 1996), p. 5-9.

[13] Fred Cohen "wrote the book" on computer viruses, through his Ph.D. research, dissertation, and various related scholarly publications. He developed a theoretical, mathematical model of computer virus behavior, and used this to test various hypotheses about virus spread. Cohen's formal definition (model) does not easily translate into "human language." See Dr. Fred B. Cohen, *A Short Course on Computer Viruses, 2nd Edition* (Wiley, 1994). Credit to Nick

note that computer viruses do not exist solely in the digital environment. For example the publication *2600*, and other magazines (published openly or underground), contain written code for viruses in a "dormant" state, waiting to be input as machine instructions in computer software.

Demonstrating the current threat from computer viruses is difficult for several reasons. In this instance, both the government and industry share a reticence to discuss and disclose "cyber-threats" and associated attacks. The government, as is common with threat estimates, has based much of its analysis on classified data. Industry on the other hand, while concerned with privacy and proprietary data, is perhaps more driven by the desire not to lose customer confidence by disclosing vulnerabilities and mishaps involving its automated information systems.

The Report of the President's Commission on Critical Infrastructure Protection (PCCIP) represents the most inclusive efforts to date to arrive at a baseline unclassified threat statement for computer networks. In addition to the "hacking threat, " the commissioners specifically mentioned America's potential vulnerability to viruses. "The threat is real enough....Skilled computer operators have demonstrated their ability to gain access to networks without authorization....Whatever their motivation, their success in entering networks to alter data, extract financial or proprietary information, ***or introduce viruses*** demonstrates that it can be done and gives rise to concerns that, in the future some party wishing to do serious damage to the United States will do so by the same means."[Emphasis added.][14] While general information on the threat from viruses is available,[15] more specific public information on deliberate attacks is unlikely to appear unless and until some of the PCCIP's recommendations for information sharing are implemented.

Our aim, though, is to explore the use of viruses as a metaphor for modern threats. In the context of our metaphor to visualize threats, what if we step back from the actual machine instructions used in computer viruses? Does the virus metaphor apply to the more common "hacking" threat? Cyber attack in the form of unauthorized entry into a network or system is a serious concern, and comprised the chief focus of the PCCIP. One of the more rigorous examinations of threat of computer attack is a 1996 General Accounting Office (GAO) report. While the report admits the exact number of computer attacks on the Department of Defense is unknown, "Defense may have experienced about 250,000 attacks last year [1995], and...the number of attacks is increasing."[16]

FitzGerald, maintainer of the VIRUS-L/comp.virus Frequently Asked Questions (FAQ) site on the Internet, for keeping this posting.

[14] *Critical Foundations: Protecting America's Infrastructures*, The Report of the President's Commission on Critical Infrastructure Protection, October 1997, p. 5.

[15] See *Computers Under Attack: Intruders, Worms, and Viruses*, edited by Peter J. Denning (ACM Press/Addison-Wesley, 1990), *Rogue Programs: Viruses, Worms and Trojan Horses*, edited by Lance J. Hoffman (Van Nostrand Reinhold, 1990) and *A Pathology of Computer Viruses*, David Ferbrache (Springer-Verlag, 1992).

[16] *Computer Attacks at Department of Defense Pose Increasing Risks*, GAO/T-AIMD-96-92 (Washington, D.C.: GAO), 22 May 1996, Chapter 2 (unpaginated).

The report relays what has become an infamous collection of statistics by the Defense Information Systems Agency (DISA). The implications are eye opening for strategists. According to the report, the DISA Vulnerability Analysis and Assessment Program simulates cyber attacks by attempting

> to penetrate computer systems at various military service and Defense agency sites via the Internet. Since the program's inception in 1992, DISA has conducted almost 38,000 attacks on Defense computer systems to test how well they were protected. DISA successfully gained access 65 percent of the time. Of these successful attacks, only 988 or about 4 percent were detected by the target organizations. Of those detected, only 267 attacks or roughly 27 percent were reported to DISA. Therefore, only about 1 in 150 successful attacks drew an active defensive response from the organizations being tested.[17]

Using part 2b of the formal definition from this paper's introduction, consider for a moment the nature of these simulated cyber attacks, as well as actual attacks reported in the news media. There are many types of hackers, who

- can be aggregated by age, motivation, nationality, etc. ("any of a large group of")
- are extremely small in relation to their targets—from one to a handful of "hackers" taking on several major military installations simultaneously for example ("submicroscopic" in relative size)
- obtain unauthorized and undesirable entry ("infectious agents')
- recruit new members, teach them, and share tools ("are capable of growth and multiplication"), and
- according to the GAO report have caused costly and considerable damage ("cause various important diseases").

Certainly the virus metaphor appears to be a fitting layman's thumbnail sketch of the cyber attack threat. On one level it can be said that infectious agents (hackers) sometimes use infectious agents (viruses) in their cyber attacks.

Cognitive Viruses: Definition and Threat Context

Perhaps the most challenging type of warfare to relate convincingly to the virus metaphor is memetic warfare. This is the case for a number of reasons. First, *memes* and *memetics* are both relatively recent terms in scholarship and national security explorations. Second, by no means are the ideas contained in and accompanying the area of memetics accepted by either academics or strategists as proven. Finally, memetic warfare is the least tangible type of warfare nominated in this paper for serious examination.

The scope and scale of this paper do not permit a full description or defense of the idea of memetic warfare. The closest related doctrinal term would be perception management, defined

---

[17] *Computer Attacks at DoD,* Chapter 2 (unpaginated).

as "Actions taken to convey and/or deny selected information and indicators to foreign audiences to influence their emotions, motives, and objective reasoning; and to intelligence systems and leaders at all levels to influence official estimates, ultimately resulting in foreign behaviors and official actions favorable to the originator's objectives. In various ways, perception management combines truth projection, operations security, cover and deception, and psychological operations."[18] Fortunately in the context of the Army After Next Project's construct, the nomination of "innovative ideas" like memetic warfare is encouraged. It is when the idea becomes a candidate for an Army concept or doctrine that it undergoes the acid test. In this paper we can, however, outline the idea and discuss it in terms of cognitive viruses.

We define a cognitive virus as any agent that infects people with a meme, a unit of information in a mind whose existence influences events such that more copies of itself get created in other minds. Professor Dawkins hinted at the original idea of the meme in his book *The Selfish Gene*, and he defined the term in *The Extended Phenotype*.[19] Several thinkers have extended this idea to discussions of warfare, including the father of modern information warfare, Dr. Thomas P. Rona, who described the idea of "societal immunodeficiency virus" (or SIV, against which unwarned populations would have no effective defenses) in some of his last discussions and writings.[20]

A good but very short (three-page) summary of the memetic warfare idea is found in the Jane's Special Report on *US Information Warfare,* by Dr. George Stein and Col. (Ret.) Richard Szafranski. The section titled "The Memetic Warfare Model" attempts to apply memetics to the topic of information warfare, with very intriguing implications. The authors first recap the tenets of memetics, describing the meme as "the basic unit of cultural imitation....the means by which a society reproduces itself." They also call memes the "monads or building blocks of culture, thinking and behavior," and state that "Humans appear to be able to create 'designer viruses" of the mind [that] nature cannot."[21]

Turning to the topic of information warfare (IW), Stein and Szafranski speculate that "IW activities would be designed to...insert new memes into the mind of the adversary. In so doing, however, the mind viruses would immediately begin to evolve as each affected enemy mind added to or modified the deployed virus." According to the authors, if borne out by further research and scientific study,

> In memetic-based IW, overt and subliminal messages could be constructed to communicate memes at multiple levels, aiming to travel at what Col. [Robert J.] Wood

---

[18] *Joint Pub 1-02*, p. 75.
[19] Richard Dawkins, *The Selfish Gene* (Oxford: W.H. Freeman, 1976) and *The Extended Phenotype* (Oxford: W.H. Freeman, 1982).
[20] See *To Challenge and Defeat the United States,* Thomas P. Rona and Gerald D. Godden, 1997, unpublished (as yet) fictional manuscript, and from this author's monthly working breakfasts/lunches with Dr. Rona in 1996 and 1997.
[21] George Stein, Ph.D. with Col. Richard Szafranski, USAF (Ret.), *US Information Warfare*, Jane's Special Report (Alexandria, VA: Jane's Information Group, 1996), pp. 145-147.

characterized as different "channels."[22] Hidden somewhere in the surrender and safe passage leaflets routinely used to incite enemies to despair and surrender ought to be a snake split in two, a good soldier towering above, an abundance of food and sunshine on the surrender side of the line and a golden bridge across. Where propaganda leaflets fail to use multiple channels, they fail to compound the probability that the right memes are communicated."[23]

We need to point out a chief difference between traditional propaganda and memetic warfare, and introduce a threat context for cognitive viruses. Unlike traditional psychological operations (PSYOP) themes and messages, cognitive viruses by our definition infect people with a meme, a unit of information in a mind whose existence influences events such that more copies of itself get created in other minds. These memes present a potential threat and opportunity for military strategists because they spread so well and are so durable. In America, civilian examples of these memes are the "bad ideas" that simply won't go away. In *Virus of the Mind,* Brodie illustrates several such as conspiracy theories (to include both "vast right-wing and vast left-wing" themes), urban legends (e.g., decades-old complaints that Procter & Gamble's logo is a satanic symbol), and get-rich-quick/Ponzi schemes that continue to draw in victims and make their propagators rich.[24]

While these examples may make for amusing coffee-bar banter, some memes have very deleterious effects with potential impacts on the overseas environment in which US national security activities (and potential military deployments) occur. During the Korean Conflict, PSYOP involving allegations of US germ warfare operations spread particularly quickly, and proved resistant to repeated US denials.[25] More recently there has been a continuous low-level strain of rumor and innuendo that the CIA and/or DoD invented the AIDS virus, and then exported it overseas as part of a racist plot. Frank Barnett writes that *glasnost* failed to inhibit "Gorbachev's regime from inciting Africans to believe that US defense factories generated the AIDS virus, or from inflaming India with the rumor that Washington hatched the plot to assassinate Mrs. Gandhi,"[26] and these particularly tenacious memes have yet to be eradicated.

For another example, we could ask soldiers who have been stationed in Latin America, specifically those who have traveled to Guatemala, about the enduring local rumors that Americans are buying babies and using them for body parts and medicinal experiments.[27] We can speculate whether some of these memes are so potent as to be impossible to eradicate, but will continue to require managed treatment when outbreaks flare up, in the form of denials

---

[22] See Col. Robert J. Wood, *Information Engineering: The Foundation of Information Warfare*, (Maxwell AFB, AL: Air War College, 1995)
[23] *US Information Warfare*, p. 146.
[24] Brodie, *Virus of the Mind*, various chapters/sections.
[25] See *PSYWAR: Psychological Warfare in Korea 1950-1953*, Stephen E. Pease (Harrisburg, PA: Stackpole Books, 1992), pp. 81, 139-142, 151-153, and *Dezinformatsia: Active Measures in Soviet Strategy*, Richard H. Shultz and Roy Godson (Washington: Pergammon-Brassey's, 1984), pp.122-123.
[26] Frank Barnett, "Reviving American PSYOP," in *Political Warfare and Psychological Operations: Rethinking the US Approach*, Carnes Lord and Frank R. Barnett, eds. (Washington: NDU Press/GPO, 1989), p. 215.
[27] Author's multiple personal conversations with Panamanian and Guatemalan enlisted soldiers and noncommissioned officers while stationed in Latin America from 1986-1988.

and focused public information campaigns. In addition we might ask what the difference is between memetic warfare and the doctrinal term of perception management. There might not be a difference; perhaps the ideas we described above are only an advanced form of modern perception management, using the best research and analysis available from area specialists, cultural anthropologists, psychologists, technologists, and communications professionals. On the other hand, it may be that memetics will enable military analysts, planners, and decision-makers the means to obtain a greater understanding of IW, providing a very potent and refined tool with which to shape our adversaries' perceptions. In that case, the effect may very well most resemble the activities of "viruses of the mind," and the virus metaphor would be well chosen.

Suitability of the Virus Metaphor

Metaphors, like loaded weapons, should be used cautiously.
Martin Libicki

Although we chose the virus metaphor to help visualize modern threats, the technique is not without its pitfalls. Martin Libicki used metaphors as intellectual tools throughout his book *Defending Cyberspace and Other Metaphors*, but he is cautious in prescribing them:

> Before analysis proceeds and policy recommendations can be justified, metaphors must be put back into the box from whence they cam so that issues can be understood for what they are, not what they look like. To use metaphor in place of analysis verges on intellectual abuse. It invites the unquestioning extension of a logic that works across the looking glass but lacks explanatory power in the real world. Those who forget this are apt to try to make their metaphors do their thinking for them.[28]

Put another way, when one holds a hammer, most problems look like nails. However, Libicki's metaphors, including a fascinating essay on warfighting lessons to be learned from observing the human immune system,[29] show an appreciation for the judicious use of metaphor.

In the "data smog" of the modern information environment, decision-makers, planners, and analysts often use only a few, highly representative pieces of information to reduce problems of current operations to a manageable size. The military leadership's emphasis on extending conceptual horizons to the year 2020 and beyond also impels strategists to conduct assessments, present recommendations, and make decisions with even less clarity and confidence in our assessments. In response decision-makers and staffs will use shortcuts, or heuristics, to classify situations according to a few key features and guide their thinking (and learning).

The virus metaphor shows some promise as a visualization tool to grapple with modern threats in biological warfare, computer network attack, and memetic warfare. Used judiciously, and in particular if coupled with the Army After Next Project's construct of doctrine/concepts/ideas, the virus metaphor helps provide both definition and context for harried strategists assembling concise threat pictures. If the metaphor withstands the scrutiny of time

[28] Libicki, *Defending Cyberspace and Other Metaphors*, p. 6.
[29] Libicki, "Postcards from the Immune System," in *Defending Cyberspace*, pp. 75-96.

and criticism, it may prove a valuable thinking and learning tool suitable for the military's intellectual toolbox.

Viruses, WMD, and Asymmetrical Warfare

For all our focus on viruses as a metaphor to visualize modern threats, how serious are "virus threats"? Are viruses really weapons of mass destruction (however unconventional)? If so, could the United States be blindsided by their employment?

Weapons of Mass Destruction. Certainly the potential exists for a "bolt out of the blue" strike comprised of biological weapons. Their delivery at the proper time and place would almost assuredly cause massive casualties in a highly industrialized nation, with estimates ranging from 100,000 to a million for more serious attacks. Efforts to control them range from international agreements such as the Biological and Toxin Weapons Convention to the contentious United Nations inspection teams trying to accomplish their mission in Iraq. Biological viruses are weapons of mass destruction in the most concrete sense, with permanent and complete effects projected to be every bit as lethal as some nuclear weapons.

Weapons of Mass Disruption. The case of computer viruses, writ small as machine instructions or writ large as hackers, is less clear. Certainly there those who predict an "electronic Pearl Harbor," a large-scale surprise information warfare strike on America's critical infrastructure. Others acknowledge this possibility, but believe the more likely circumstance to be a large-scale attack without very destructive effects. For a strategic cyber attack, the "modern version of the *scorched earth principle becomes logically the destruction, incapacitation and corruption of the enemy's information infrastructure.* This aspect of 'information warfare' has the side benefit for the attacker to create confusion, panic and irrationality among the civilian target population...."[30] In this case, viruses are more like weapons of mass disruption, having a temporary and partial, albeit it potentially serious effect. (See Figure 2)

Weapons of Mass Deception. Finally we turn to the question of cognitive viruses. While some may abhor their use in either peace or war, their employment seems destined to continue, if not increase. It has been argued that what we have called memetic warfare has been used to instigate outbreaks of extreme violence in Rwanda, Somalia, and the former Yugoslavia. The issue is highly inflammatory, but the misuse of mass media is sufficiently troubling that recommendations to create a special UN unit to "monitor, counter, and block radio and television broadcasts that incited widespread violence in crisis zones around the world" has come from such unlikely sources as a former U.N. Human Rights Officer.[31] However troubling the concept of cognitive viruses might be in some quarters, and recognizing that they can exacerbate if not instigate bloodshed, they are better termed weapons of mass deception than mass destruction.

---

[30] Thomas P. Rona, "From Scorched Earth to Information Warfare," in *Cyberwar: Security, Strategy, and Conflict in the Information Age*, Alan D. Campen, Douglas H. Dearth, and R. Thomas Goodden, eds. (Fairfax, VA: AFCEA International Press, 1996), p. 10.

[31] Jamie F. Metzl, "Information Intervention: When Switching Channels Isn't Enough," in *Foreign Affairs*, November/December 1997, p. 15.

Rather than thinking of them solely in terms of WMD, a better approach is to recognize that the different types of "virus warfare" are well-suited for use as asymmetrical means in a conflict. Asymmetrical warfare, a current focus of discussion in military strategy circles, likely represents the probable challenges the US will face in future conflicts. As General Charles Krulak summarized, "Our enemies have seen CNN. They watched the technology and they will not be content to fight the son of Desert Storm. They will fight the stepson of Chechnya, the stepson of Somalia. [The 21st century] will be a century—the first part of it at least—of chaos."[32]

Assessments of Army After Next wargames have supported the General's assessment. Asymmetrical responses characterized the Red Team's response in the face of Blue's superiority in firepower and information dominance. "Red's learning curve rose sharply as the games progressed. Confronted by overwhelming combat power, he resorted to asymmetric responses in an effort to offset Blue's advantages."[33] Just as the notional adversaries engaged in asymmetrical warfare during the wargame, future US adversaries similarly could employ the three types of "virus threats" described above. Thinking through the implications of asymmetrical threats, using the virus metaphor to visualize them, could assist strategists in this difficult task.

---

[32] John Archibald, "Top Marine: Don't fight yesterday's wars in 2000," *Birmingham News* (Alabama), 3 December 1997, p. B1.

[33] *The Annual Report on The Army After Next Project to the Chief of Staff of the Army*, July 1997, p. 14.

Figure 1: Viruses in the Context of Warfare

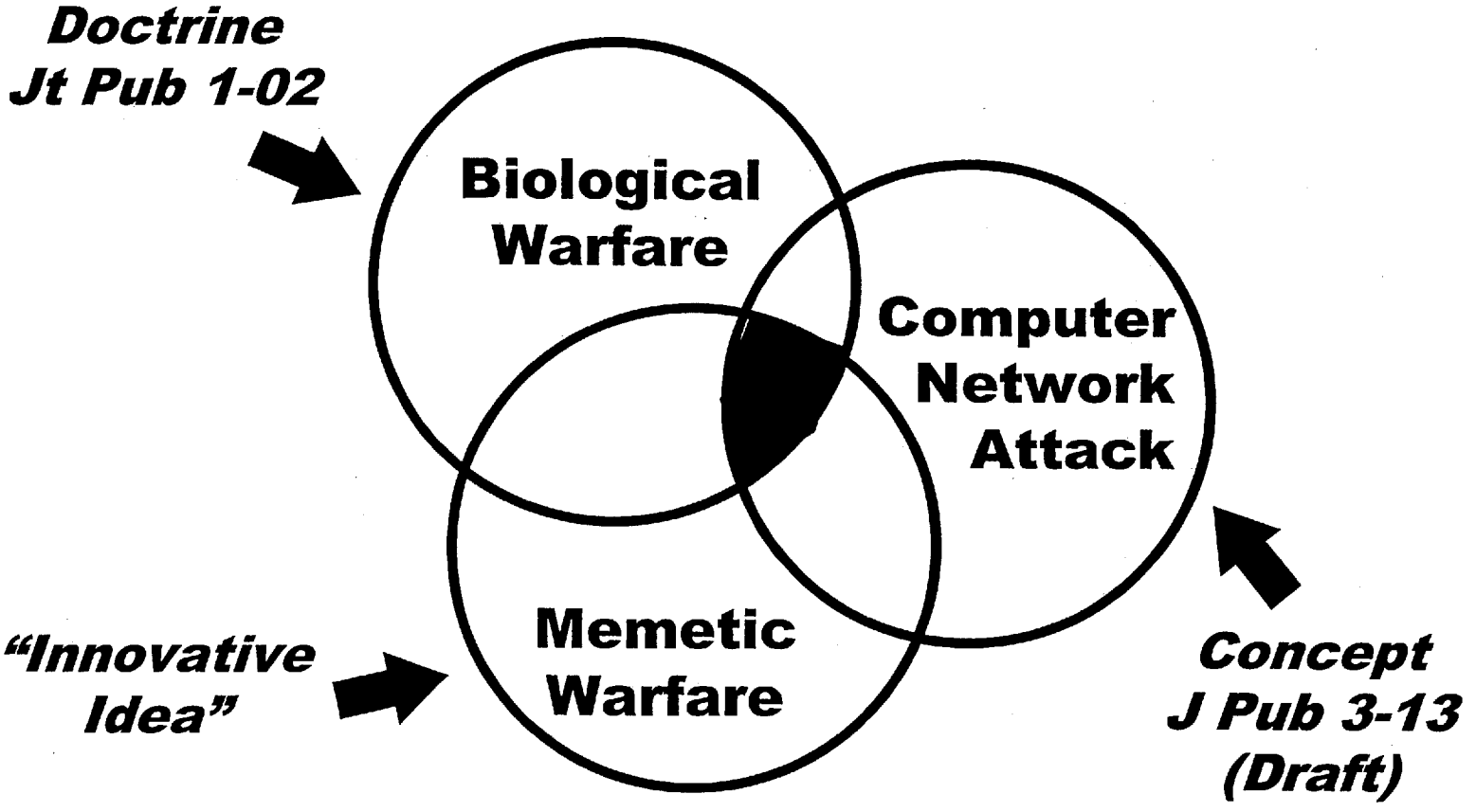
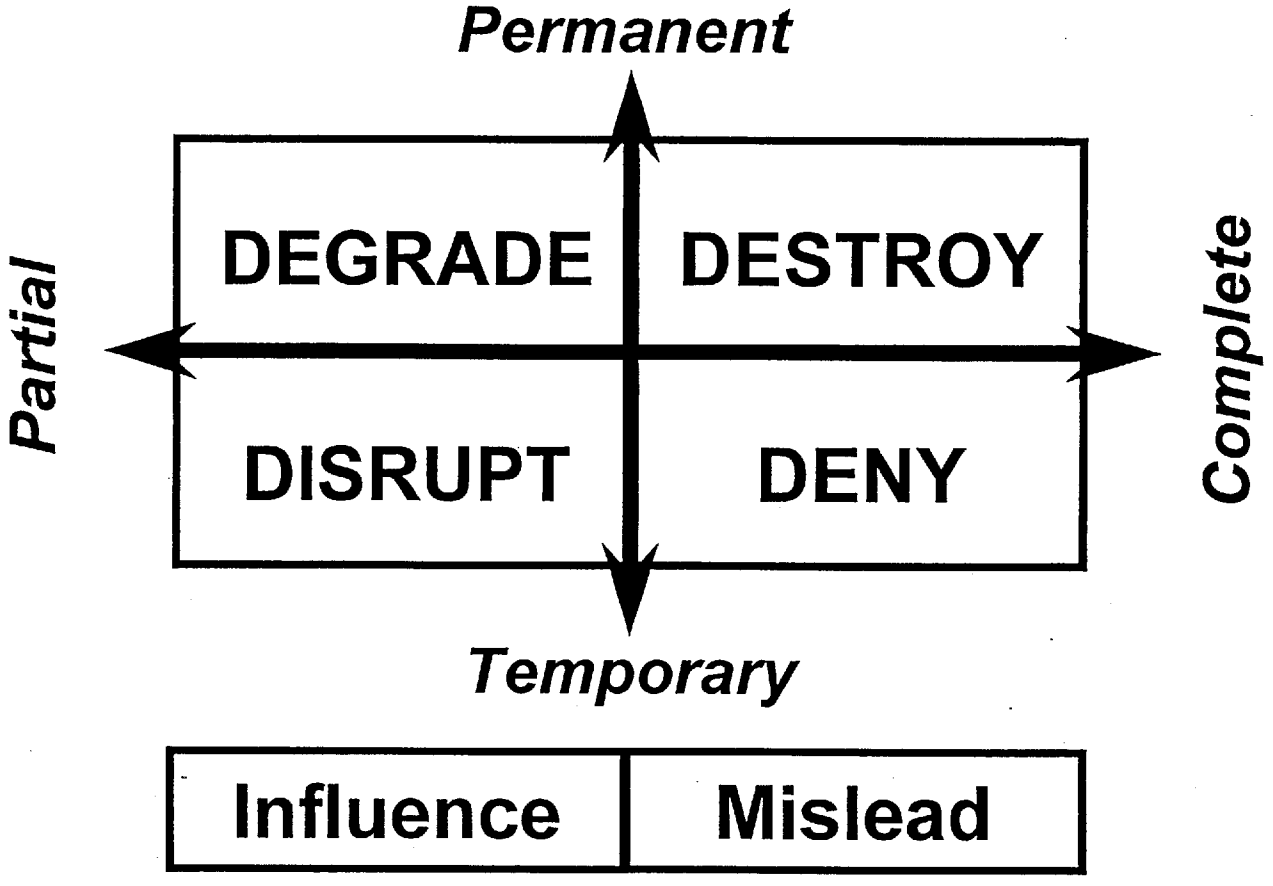


Figure 2: Unconventional Weapons of Mass Destruction?



///

PROCEEDINGS 1998 7th International Conference & Exhibit OPEN SOURCE SOLUTIONS: Global Intelligence Forum - Link Page

Previous	Transnational Enemies
Next	Takedown: The Asymmetric Threat to the Nation

Return to Electronic Index Page