The US Army War College Quarterly: Parameters

Volume 26
Number 4 *Parameters Winter1996*

Article 12

11-7-1996

Deterring Information Warfare: A New Strategic Challenge

Timothy L. Thomas

Deterring Information Warfare: A New Strategic Challenge

TIMOTHY L. THOMAS

From *Parameters*, Winter 1996-97, pp. 81-91.

> "We are now seeing a tendency toward a shift in the center of gravity away from traditional methods of force and means of combat toward non- traditional methods, including information. Their impact is imperceptible and appears gradually. It is less burdensome economically and is not dangerous ecologically. . . . Thus today information and information technologies are becoming a real weapon. A weapon not just in a metaphoric sense but in a direct sense as well."[1]

In 1995, a 28-year-old Russian biochemistry graduate student in St. Petersburg, Vladimir Levin, used sophisticated computer codes more than 40 times to break into New York Citicorp's computerized cash-management system. He transferred more than $12 million to banks around the world and had access to Citicorp's daily transfer of $500 billion. Only the cooperation of the FBI, Russian police, and law enforcement agencies on four continents prevented a catastrophe and eventually resulted in Levin's arrest.[2] Levin's "cybercaper" underscores the vulnerability of sensitive economic (and by analogy, defense) systems to computer hackers operating from terminals located anywhere in the world. An attack on any economy or defense structure conceivably could be initiated by any foreign government or hostile threat without forewarning or even physical evidence that it had occurred.

Rapid technological change presents a specific new challenge to strategists: the requirement to master the emerging forms and functions of information technologies. New developments in managing information can create suspicion--even paranoia--among nations that lack the enabling technologies we take for granted. Technologically antiquated nations, those without as well as those whose infrastructures are outdated, could be more inclined to preemptive behavior when they perceive a threat than would those states more attuned to the capabilities and limitations of the latest technologies. Whereas once the launch of nuclear-tipped missiles might have required minutes to detect, today's information assault could be completed in seconds--and remain undetected until its consequences become painfully apparent.

Strategists and policymakers need to explore issues such as "information assault" because the genie is out of the bottle; we cannot ignore the fact that technology generally considered benign can be turned against another state with devastating consequences. Decision by indecision is not an option in exploring the ways in which our infrastructure and our armed forces have become dependent on the new technologies. Failure to treat information assault as a potential threat could mean that some will sit idly by until there is a catastrophe. One Russian theoretician warned of such a possibility:

> From a military point of view, the use of information warfare means against Russia or its armed forces will categorically not be considered a non-military phase of a conflict, whether there were casualties or not . . . considering the possible catastrophic consequences of the use of strategic information warfare means by an enemy, whether on economic or state command and control systems, or on the combat potential of the armed forces, . . . Russia retains the right to use nuclear weapons first against the means and forces of information warfare, and then against the aggressor state itself.[3]

Confidence-building measures suitable to an era of potential information-based assaults on other states could draw initially on concepts from the nuclear age, primarily those of deterrence and non-proliferation. The concepts would have to be altered to meet the challenge of an assault that can cripple a national banking or telephone system without leaving physical evidence of its occurrence. Other nuclear age ideas which may be of some utility include launch under attack, preemption, and the application of crisis management methodologies.

This article explores the idea of deterring information-based assaults.[4] It defines the concept of an information assault and describes and explores the need for forms of deterrence tailored specifically to the threat posed by the use of electronic means as weapons. A companion piece, "The Possibilities for Mutual Deterrence: A Russian View" by a Russian officer who specializes in strategic intelligence, gives another perspective on the issue.

What Is the Threat?

According to the February 1995 edition of the National Military Strategy of the United States, one of the goals of the strategy of flexible and selective engagement is to "win the information war" (that is, in case of a conflict; there is no intent to imply that an information war is ongoing in peacetime). The working dictionary of the National Defense University's School of Information Warfare and Strategy defines information warfare as:

> Actions taken to preserve the integrity of one's own information systems from exploitation, corruption, or destruction while at the same time exploiting, corrupting, or destroying an adversary's information systems and in the process achieving an information advantage in the application of force. It is also actions taken to achieve information superiority in support of national military strategy by affecting adversary information and information systems while leveraging and defending our information and information systems. Command and control warfare is a subset of information warfare.[5]

Martin Libicki of the National Defense University has written a helpful description of the various types of information warfare. Aimed against military forces and state infrastructures are:

- *C2 warfare*, attacks on our ability to generate commands and communicate with the services and deployed forces
- *electronic warfare*, techniques that enhance, degrade, or intercept flows of electrons or information
- *intelligence-based warfare*, integration of sensors, emitters, and processors into reconnaissance, surveillance, target acquisition, and battlefield damage assessment systems
- *psychological warfare*, designed to affect the perception, intentions, and orientations of decisionmakers, commanders, and soldiers
- *cyberwar*, the use of information systems against the virtual personas of individuals or groups
- *hackerwarriors*, who use their techniques to destroy, degrade, exploit, or compromise information systems
- *economic warfare*, expressed in one of two forms: as an information blockade (which presumes that information flows are as important as supply flows) or as information imperialism (which presumes one believes that trade is war) [6]

Each type of warfare described by Libicki would require its own rules of engagement, based on its methods, objectives, and technologies. It is essential to use the leverage attained from modern reconnaissance and intelligence collection systems to "assure that this leverage works for us and against our adversaries." FM 100-6, *Information Operations*, goes further, citing the need to acquire, use, protect, exploit, deny, and manage information activities. In accordance with the desire to win the information war, information assets are now strategic assets, and should be so reflected in our national security policy. The primary threat to US and Russian information systems and the data they contain and process, then, would be an adversary's ability to alter, replace, or delete the information stored or generated by these systems and to influence the processes by which it is managed.

Threat Subsets

Advanced information technologies are required if one is to disrupt the integrity of information systems and defeat an opposing force or damage a state infrastructure through information warfare. *These technologies represent one aspect of the threat to all nations*. They most readily appear today in the form of satellite surveillance systems, global navigation systems, and commercial communications and satellite systems. These systems are presently experiencing some leveling among nations possessing the technologies, because the United States, Russia, France, and China are more willing to share them with others than at any time in the past. This change in national policies is due primarily to two phenomena: the end of the Cold War, and the trend to develop jointly the ecological monitoring systems that are needed to help prevent global contamination or depletion of natural resources. Nevertheless, the US desire to slow the

spread of these technologies is apparent:

> Precise navigation and imagery in the wrong hands can imperil US forces. Space-based communications reduce the US advantage in military command and control. Cryptographic capabilities could permit terrorists to plan havoc undetected. Space launch capabilities can lead to ballistic missile proliferation that destabilizes regions.[7]

Information gathered, stored, and used by those who possess such technologies knows no boundaries, recognizes no sovereignties, and is hardly covered by international law. Consequently, it has become much more difficult to identify when a country or region is under attack or when national sovereignty has been breached. How does one appeal to the UN when that organization's charter does not allow the collection of intelligence, which in many cases is simply the collection of information? *Another element of the threat, then, is the absence of legal mechanisms,* agreed to by the international community, that could provide coherence to the many commercial and government decisions made in the information area. For example, what should be considered by law as an information assault? Is it an information strike, an information embargo, information theft, or all of these in varying proportions? One US strategic assessment noted:

> Government policy decisions do affect the precise direction in which information technologies advance, the channels through which they are allowed to flow, and the speed at which they spread from the technologically advanced nations to other societies . . . . From a national security perspective, the most salient trend in the new information environment is that the capabilities that DOD spent billions to build in the 1980s are increasingly available for other nations to buy or rent at a fraction of that cost.[8]

The absence of international agreements that could regulate the use or denial of data and information, and the rapid development of information technologies, give rise to a *third element of the threat: the emergence of new methods to manipulate perceptions, emotions, interests, and choices* and thus serve as a psychological weapon. This is not the overt psychological operation of the past that juxtaposed one system of values or beliefs against another. It is instead a razor-sharp weapon that manipulates emotions and perceptions through any mass medium--radio, TV, the Internet, or the press--separately or in varying combinations. This weapon can contaminate through manipulation ranging from tainted sources, skewed historical understanding of the complexity of a situation, or policy entanglements within a government apparatus during a transition period, to targeted monetary support of factions in a nation or region.

The most obvious carryover from the Cold War period is radio and television broadcasting, which knew no borders then and knows no borders now. News reported on CNN or other networks, immediately accessible by politicians all over the globe, can cause a flurry of diplomatic activity if reports contradict positions taken in private, or if they appear somehow to influence those decisions. General Colin Powell's use of CNN to stay abreast of damage assessment during the initial stages of the Gulf War is a good example of being able to "see what we know in real time." Even a modest ability to influence decisions can have unpredictable consequences and therefore must be considered as an element of the threat. The ability to control such information, had it been in the hands of Saddam Hussein instead of the United States, could have produced entirely different results. As a Russian information warfare specialist noted,

> The introduction of information totalitarianism has now become the norm in international relations. The growing influence of the mass media on the course and substance of political processes and the functioning of governmental mechanisms is one of the dominant trends in the development of contemporary society.[9]

This same specialist foresaw two other kinds of problems for Russia. The first kind includes the loss of valuable information, such as the disclosure of state secrets, special eavesdropping measures, or the use of medical, chemical, or other agents to influence people's thinking. The second identifies the introduction of false data into information systems.[10]

A fourth element of the threat is the speed with which information assaults can be conducted, giving little time for crisis managers to respond. In the past there were early warning systems to give indications of enemy intentions or launches, and some measurable delay between initiation of the assault and its culmination. Now, events can occur almost instantaneously and often without detection. These emerging capabilities can encourage suspicion, paranoia, and a willingness to consider preemptive strikes.

A final information threat is simply the availability of masses of information to anyone who wants it. Information once denied to terrorists or criminals is now available to them in highly usable forms. Legitimate on-line services allow individuals to request information about a diverse series of topics (e.g., how to make a nuclear weapon, weapon blueprints, outline and defense of a border region) from universities or other data banks. Information that once took years of research to assemble now can be acquired in a matter of seconds. It is far more dangerous in the hands of terrorists today than it would be in the hands of more conventional adversaries, whom one expects would fully understand the consequences of using it to support aggressive behavior. This situation can encourage collaboration between hostile governments and non-state actors of all kinds to develop and carry out with relative impunity operations against the United States, its allies, and its friends. Information still denied to unauthorized users can be obtained by persistent hackers, operating on their own or under the sponsorship of a state or rogue organization.[11]

Why Deterrence?

According to US Joint Publication 1-02, deterrence is "the prevention from action by fear of the consequences. Deterrence is a state of mind brought about by the existence of a credible threat of unacceptable counteraction."[12] The key element of the February 1995 National Military Strategy is nuclear deterrence. At the time that document was drafted, however, there seemingly was no emphasis on information warfare as a prospective threat and hence no inclination to address it by name in the same context as the better-known nuclear threat. Thus the highest priority of our military strategy at this writing is to deter a nuclear attack against our nation and allies. Our survival and the freedom of action that we need to protect extended national interests depend upon strategic and nonstrategic nuclear forces and their associated command, control, and communications.[13]

Increasingly, however, the power of information technologies allows any country to limit the survival or freedom of action of another through the control or corruption of data and information, or through the development of new information technology. As a result it is in the interest of the United States to codify an international legal position on the use of these technologies, especially as they can be used to gain a strategic advantage over other states.

Defining Deterrence Against Information Assault

A suggested definition of deterrence against an information assault is this: The ability through international law, specific applications of information technologies, or the monitoring of "perception management" to deter an information assault on the territory of a sovereign state. The term "territory of a sovereign state" includes the airwaves and information channels above, around, and below the territory in question. It includes transnational relations between and among states that would be affected by an information assault on the social structures of the state, on its economic or political functions, such as its financial markets, or on industry or infrastructure, such as power grids or communication systems.

Deterrence against information assault is required today, particularly to alleviate concern over the rapid application by some nations of information technologies and the implications of an expanding gap between those who possess the technologies and those who don't. Systems such as the Internet have proven their utility to those with access to them; they can also produce genuine fear among strategic thinkers of states that do not possess them. Several noted Russian scientists recently observed:

> These fears are primarily associated with the problems of guaranteeing the security of national information resources [and] telecommunications, and [with] the prevention of computer crimes. These problems are especially urgent for countries in which the creation of their own information infrastructure is lagging and which do not have adequate resources to either resist this new American initiative or to join the superhighway as equals. Russia is among those countries.[14]

Russia has been at the forefront of theoretical attempts to harness this technology, through joint conferences and organizations, before it spins out of control. Russian military and technical scientists have constantly called for joint seminars, and have even developed the International Information Academy to serve as a global networking system of information systems and thinkers.[15] Through these and other such forums they have called for the immediate start of international cooperation on information technology issues. Three Russian scientists specializing in information

security issues observed recently:

> The international cooperation that is needed to cope with the prospects of misuse or abuse of information systems should focus on the development and adoption of legal provisions and agreements that guarantee information security in cross-border information exchange processes. Specifically, measures of an international character that are directed at preventing, or failing that, ensuring liability for computer crimes, must be defined and juridically reinforced.[16]

There is a problem, however, with the concept of deterring information assault. Unlike the threats associated with nuclear weapons during the Cold War--where control was tight and exercised by governments--information weapons (the computer virus, intrusion into sensitive systems) can be used by any hacker with the competency to enter a government, corporate, or individual net. Control over information and the systems that produce it is not centralized; neither is it the near-complete monopoly of government that defined the systems of deterrence during the nuclear age. Therefore the means to detect, control, and respond to such intrusions need to be developed far beyond those required by the nuclear threat.[17]

The Means to Deter Information Assaults

The fundamentally different problem of deterring information assault is created by the large number of people with the means, the skills, and the will to disrupt information in storage or in transit. Nuclear proliferation for decades was hindered by the difficulties inherent in acquiring the means and the skills to create a nuclear weapon. These difficulties created de facto government nuclear monopolies. This is no longer the case; computer hackers sitting in the privacy of their homes can damage information systems anywhere in the world.

Factors that can put deterrence of information assault into context as a priority issue include:

- Governments could intimidate and pressure other governments with information warfare just as they did with nuclear weapons, except that collateral damage in the physical sense will not be as great. This circumstance probably enhances for some regimes the appeal of using information warfare.
- Just as a few superpowers once sought nuclear parity, now many nations will seek parity in the realm of information technology. There is nothing to stop any nation from sponsoring domestic or imported hackers in acts of aggression in the quest for parity.
- Monitoring of technological advances that can facilitate information assault should become a priority issue throughout the world. This includes the realms of theoretical and applied science, the prerequisites and conditions for possible employment of the resulting new technologies, and predictions of global or local conditions or conflicts that may carry with them the threat of information warfare.[18]

Several methods of deterring information assault present themselves. The first is the legal aspect, defined by what the international community will consider as an information attack on a sovereign state, or by what one state should consider as an unlawful intrusion into a domestic information system. Without such a concept, a seemingly harmless application of information technology by one state may be considered to be an attack by another and could lead to serious escalation.

Second, the information component or potential of a weapon is the portion of a weapon that uses information technology (digitalization, miniaturization of control systems) to increase the weapon's lethality and accuracy. Agreement to limit the capability of this potential may be another form of deterrence in the information age. Cannon artillery, which still relies on technology and procedures from World War I, will never have the information component possessed by today's multiple launch rocket system.

Third, it would seemingly be wise to institute some type of information early warning system, not of the type to handle incoming information attacks of which one might not be aware, but rather a sort of crisis management early warning system to handle potential or actual strikes once detected. This would offer a method to respond through international organizations to actual or simulated attacks, and could help distinguish between the two. Obviously, this also will require stricter checks on individuals (more two-person controls on access to critical systems or databases) since one person now has the potential--through manipulation of information networks--to inflict destruction on a scale once

imaginable only through an electromagnetic pulse or a neutron weapon.

Finally, the growing business of transnational relations may itself have a deterrent effect. Targeting of specific objects becomes more difficult as world communities and systems continue to network. An assault on a neighbor's systems theoretically could affect the assaulter's own systems if they are connected in any way to the object of the assault. In this sense, transparency and cooperation become stronger deterrents than they are for nuclear deterrence.

A Russian officer at the General Staff Academy noted recently that "the armed forces of likely adversaries are in a state of constant information warfare, and military informatics works to accomplish tasks characteristic of war even in peacetime. Electronic warfare is being waged continuously. For example, the Pentagon is guided by the motto, `Electronic warfare is declared by no one, never ceases, is waged covertly, and knows no borders in space and time.'"[19] International agreements regarding the deterrence of information assaults may be the best, if not the only, way out of this dilemma.

Conclusions

Processes such as analyzing national security issues, developing new technologies or equipment, and fielding the results of research that once took months or years now can be completed literally in days. These processes, whether applied to specific weapon systems, or employed themselves in a hostile manner, can alter not only the military aspect of national security but also the entire infrastructure of a state. New technological developments and subsequent uses of information have resulted in innovations and weapons the employment of which can have consequences comparable to those of nuclear weapons, without the attendant physical destruction. The effects of new technologies on the accumulation and use of information are unquantifiable. *Newsweek* columnist Steven Levy aptly described the power of the information revolution:

> The revolution has only just begun, but already it is starting to overwhelm us. It's outstripping our capacity to cope, antiquating our laws, transforming our mores, reshuffling our economy, reordering our priorities, redefining our workplaces, putting our Constitution to the fire, shifting our concept of reality and making us sit for long periods in front of computer screens while CD-ROM drives grind out another video clip. . . . A computer gives the average person, a high-school freshman, the power to do things in a week that all the mathematicians who ever lived until 30 years ago (1965!) couldn't do.[20]

This article has posed questions about the need for agreed definitions and legal norms related to information assault and its deterrence. Without the development of such a concept, the information threat, not at all obvious to the casual observer, can continue to proliferate. This circumstance is reflected in the apparent lack of serious discussion, legislation, or legal methods to deal with the spread of information technologies to terrorists and criminals, and in the ability of psychological operators to manipulate both world and national opinions through the advanced application of the information medium.[21]

It is appropriate to think of information technologies as comparable to nuclear technologies. While not as overtly destructive, information technologies have the potential to affect--silently and without notice--government, social, business, and financial institutions, as well as command, control, and communications systems. Any of these societal attributes may be contaminated or destroyed without the widespread physical destruction that accompanies the use of nuclear or conventional weapons. In the hands of irrational decisionmakers or rogue actors, information technologies and capabilities could prove to be as destructive to state sovereignty and the well-being of the citizens of any state as the kind of armed assault feared during the Cold War.

NOTES

1. Yevgeniy Korotchenko and Nikolay Plotnikov, "Information is also a Weapon: About what should not be Forgotten When Working with Personnel," *Krasnaya Zvezda*, 17 February 1994, p. 2.

2. William M. Carley and Timothy L. O'Brien, "How Citicorp System Was Raided and Funds Moved Around World," *The Wall Street Journal*, 12 September 1995, p. 1.

3. V. I. Tsymbal, "Kontseptsiya `Informatsionnoy voyny'" (Concept of Information Warfare), speech given at the Russian-US conference on "Evolving Post-Cold War National Security Issues," Moscow 12-14 September 1995, p. 7.

4. Another recommended name for the concept is "information-incursion impediment" or "I cubed," which may be more meaningful to the military mindset.

5. "Definitions for the Discipline of Information Warfare and Strategy," School of Information Warfare and Strategy, National Defense University, Fort Lesley McNair, Washington, D.C., p. 37.

6. Martin C. Libicki, "What is Information Warfare?" Center for Advanced Concepts and Technology, National Defense University, August 1995. The entire pamphlet is devoted to identifying and describing the seven forms of information warfare posited by Libicki. See especially pp. 7-8 and 87-89.

7. "Strategic Assessment 1995: U.S. Security Challenges in Transition," National Defense University, Institute for National Strategic Studies, p. 155.

8. Ibid., p. 151.

9. Aleksandr Pozdnyakov, interviewed by Vladimir Davydov, "Information Security," *Granitsa Rossii*, September 1995, pp. 6-7, trans. in FBIS-UMA-95-239-S, 13 December 1995, pp. 41-44.

10. Ibid., pp. 42, 43.

11. See, for example, Richard J. Harknett, "Information Warfare and Deterrence," *Parameters*, 26 (Autumn 1996), 93-107.

12. Joint Publication 1-02, "Department of Defense Dictionary of Military and Associated Terms," 1 December 1989, p. 113.

13. John M. Shalikashvili, *National Military Strategy of the United States of America* (Washington: Joint Chiefs of Staff, February 1995), p. 10.

14. Georgiy Smolyan, Vitaliy Tsygichko, and Dmitriy Chereshkin, "A Weapon That May Be More Dangerous Than a Nuclear Weapon: The Realities of Information Warfare," *Nezavisimoye Voyennoye Obozreniye*, 18 November 1995, supplement No. 3, pp. 1-2, trans. in FBIS-UMA-95-234-s, 6 December 1995, pp. 31-35.

15. The Russians have developed an information networking system that links nodes within Russia and throughout the world. It is called the International Information Academy. The Academy has over 250 functional and regional departments in Russia, the Commonwealth of Independent States, Europe, Asia, and America, where about 5000 of its full and corresponding members are working. Staffs are in Moscow, Washington, New York, Riga, Kazan, and San Diego. Over 150 members of the Russian Academy of Sciences and other national academies of the world, 70 Lenin Prize Winners, and about 400 State Prize laureates are members from Russia. Joseph Reed, Under Secretary General of the United Nations, opened the last large Information Forum in Moscow in November 1994 along with Moscow Mayor V. M. Luzhkov.

The Academy in Moscow is composed of institutes for the Study of Information, Information Linguistics, Information Mathematics, Information Philosophy, and of Information and Computer Center for User Groups (Data Sharing). Other international organizations include the Academy of Information and of Information Science, the Institute of Information and Market Relations, the Technical Center for Problems in Bionics and Computer Modeling, the Northwest Institute of Management, the Center of Legal Information, and the International Institute of Informatization. The Russian Institute of the Family and the Russian University of Information are also part of this effort.

The Academy conducted plenary meetings in 1994 for nine congresses: The World of Information, the Individual, and Society; Mass Media in the Modern World; Information and Business; Socio-Humanitarian, Natural-Science, and

Practical Problems of Information; Informational Processes and Technologies, Systems, Means of Communication, and Networks; United Information-Honeycomb Space of the World Community; Traditional and Folk Medicine, the Development of Latent Potentialities of Man (that is, parapsychology, psychotronics, etc.); the Search for Extra-Terrestrial Civilizations; and Information, Human Rights, Freedom, and Personal Security of Man in Society.

16. Georgiy Smolyan, Vitaliy Tsygichko, and Dmitriy Chereshkin.

17. The author thanks Major Donna Schutzius, US Air Force Academy, for this suggestion and for her review of this article.

18. Georgiy Smolyan, Vitaliy Tsygichko, and Dmitriy Chereshkin.

19. Ibid.; Pozdnyakov.

20. Steven Levy, "Technomania," *Newsweek*, 27 February 1995, pp. 25-29. Levy specializes in new technology for *Newsweek*.

21. For a further discussion of this phenomenon, see "International Conflict Controllers: Manipulators or Manipulated? " by Timothy L. Thomas, to be published in Low Intensity Conflict and Law Enforcement, Vol. 4 (Winter 1995).

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 7 November 1996. Please send comments or corrections to carl_Parameters@conus.army.mil.