The US Army War College Quarterly: Parameters

Volume 26
Number 3 *Parameters Autumn 1996*

Article 9

8-21-1996

Information Warfare and Deterrence

Richard J. Harknett

Recommended Citation
Richard J. Harknett, "Information Warfare and Deterrence," *Parameters* 26, no. 3 (1996), doi:10.55540/0031-1723.1791.

Information Warfare and Deterrence

RICHARD J. HARKNETT

From *Parameters*, Autumn 1996, pp. 93-107. .

The essence of the Information Age is the emergence of a new form of organization. The information technology network seamlessly connects all of its parts, creating shared situational awareness throughout an organization. High connectivity supports both enhanced sustainability and greater accessibility.

Information warfare is best understood by focusing on the concept of connectivity as both a societal and military asset. For strategists seeking to deter this new form of war, connectivity is a double-edged sword. Deterrence requires that the capability to inflict retaliatory costs be perceived as reliable. Deterrence weakens to the degree that the deterrent capability can be contested by a challenger through degradation or avoidance. The inherent accessibility of information technology invites challenges to a network's connectivity. Deterrent threats relying on such connectivity will be susceptible to technical, tactical, and operational contest. The contestability of connectivity will make deterrence of information warfare difficult. This article concludes that deterrence models developed during the Cold War will provide poor guidance for strategic thinking about this new form of war, which is better understood in the context of offense and defense.

Information Warfare

There is as yet no consensus about the term information warfare.[1] The US Department of Defense's definition as of March 1995 is remarkable for its lack of specificity: "Information Warfare is `action taken to achieve information superiority in support of national military strategy by affecting an adversary's information and information systems, while leveraging and protecting our own information and information systems.'"[2]

This phrasing is amorphous and loose enough that the strategic visions it describes are ones with which Sun Tzu or Attila the Hun could feel comfortable.[3] While the assumption is that we are talking about the employment of high technology, the DOD definition does not require it. In March 1993, Memorandum of Policy Number 30 (MOP 30), issued by the Chairman of the Joint Chiefs of Staff, identified seven different concepts to be grouped under the umbrella of information warfare. Of these, some, like command and control warfare (C2W), intelligence-based warfare, and psychological operations, do not necessarily involve information technology. Defense analyst Martin Libicki has concluded that currently the term is "an unfortunate catch-all phrase."[4]

If the term "information warfare" is to be conceptually useful, as a foundation for both strategy and analysis, it must capture some unique aspect of conflict not covered by previous terms. (If we don't apply this standard we simply raise the possibility of creating greater analytical confusion by developing unnecessary concepts.) One area of consensus does seem to exist around the idea that information warfare can be divided into two general categories: that which involves strictly military forces, and that encompassing society at large.[5] What is missing in the evolution of this definition is a degree of conceptual clarity that comes about when an organizing principle is identified.

In the case of information warfare, greater definitional rigor may be achieved by recognizing that what is truly distinctive about the Information Age (and potentially revolutionary) is the emergence of a new form of organization. The functional hierarchy and centralized decisionmaking of the bureaucratic organization, which dominated the Industrial Age, may be giving way to the shared global and situational awareness of what might be termed the information technology network. The US Army's "Force XXI" project, which has as its goal the creation of a 21st-century Army, resembles much of what might be theorized as a networked form of organization. Brigadier General

Joseph Oder, director of the Digitization Special Task Force, argues that "land force dominance does not lie with the *sequential* application of each objective but with the synergy created through the *simultaneous* application of modernized systems." This is to be accomplished through digitization, which Oder defines as,

> the application of information technologies to acquire, exchange, and employ timely digital information throughout the Battlespace, tailored to the needs of each decider (commander), shooter, and supporter, allowing each to maintain a clear and accurate vision of the Battlespace necessary to support planning and execution.[6]

The major consequence of such digitization goes well beyond a simple firepower force multiplier. It promises to provide "shared situational awareness."[7] In such an environment, information dominance truly becomes the arena of great contest for it means that advantage in knowledge about location could prove decisive, given the precision and destructive potential of modern weaponry.

The information technology network, in theory, functions on the basis of connections between nodes, which can be individuals at computers, several workstations, or small networks themselves. The strength of the network therefore rests primarily on its degree of connectivity, not on its individual nodes. In military terms it is the essence of the network--the idea of connectivity--that appears as the critical target. If we apply the conceptual construct of network connectivity to the two general categories mentioned above, we may develop a clearer definition of information warfare: one in which *connectivity on the battlefield* and *societal connectivity* are the focuses.

John Arquilla and David Ronfeldt have identified two discrete types of information warfare: netwar and cyberwar. While a good starting point, both terms can be given greater precision by recognizing the importance of two phenomena: organizational change as the basis of the information revolution and the idea of connectivity itself. Arquilla and Ronfeldt define *netwar* as "information-related conflict at a grand level between nations or societies. It means trying to disrupt, damage, or modify what a target population knows or thinks about itself and the world around it." *Cyberwar* "refers to conducting, and preparing to conduct, military operations according to information-related principles. . . . It means turning the `balance of information and knowledge' in one's favor." It signifies a "transformation in the nature of war, [but] . . . does not necessarily require the presence of advanced technology."[8]

Netwar

If we begin with the presumption that what is potentially revolutionary and distinctive about the Information Age is the emergence of the network organizational form and the attendant importance of connectivity, both of these terms can be sharpened. Arquilla and Ronfeldt place netwar in the context of a competition over ideas. As they present it, the target is information itself, or more specifically, knowledge. In this sense, the term seems to resemble closely what might be considered sophisticated propaganda warfare.

Arquilla and Ronfeldt agree with the notion that the information revolution has more to do with organization than information, but they fail to capture this in their netwar definition. The refinement offered here is that the term netwar primarily refers to *attacks on or defense of societal connectivity.* That is, netwar refers to information-related conflict at a grand level, which involves attempts to destroy an enemy's societal connectivity and protect one's own. The target range includes a society's communication, financial transaction, transportation, and energy resource network links. While degradation and protection of physical assets are important, the primary focus is on attacking and defending the linkages essential to the functioning of modern society. Again, there is no reason to develop new conceptions of warfare if all we are talking about is competing for the hearts and minds of people. Propaganda and psychological warfare cover that realm.

The concept of netwar is useful only to the degree that it conveys a new form of warfare. To consider societal connectivity a useful target, a society must be dependent enough on these networks to make their loss important. Thus, nomadic, feudal, or even moderately industrialized societies that show little signs of network characteristics are not likely targets for offensive netwar operations. Arquilla and Ronfeldt posit that neither netwar nor cyberwar (discussed below) requires high technology. In this, they and others leave open the door for employing high-tech information warfare tactics against low-tech societies. While they are correct that information warfare is not simply about high-tech weapons, they overlook the point that the emergence of organizational change--the emergence of the network--is a

result of the information technology revolution. Thus, where that revolution has not taken hold, societal connectivity as the term is used here is likely to be low, making the concepts of netwar and cyberwar considerably less useful for thinking about conflict.

The RAND Center for Information Revolution Analyses published a general scaling of worldwide connectivity for 1995. They used the basic presence of e-mail networks as the measure of connectivity. Employing a scale of 0 to 16, where 16 was high connectivity, they found that much of Africa had zero connectivity and most of the Middle East and Southeast Asia would receive no more than a 4 rating.[9] While computer communications is not the only measure of societal connectivity, it is critical. In terms of the pervasiveness of the network form, the presence of information technology is key. Where it is not present, capture or destruction of the *single* radio-television station can produce great effect. Here, the hierarchical form still dominates, decapitation is possible, and traditional operations--conventional, propaganda, and psychological--are sufficient. While decapitation certainly can lead to the severing of ties between central authority and society at large, it is centralized control that is the target.

In an emerging networked society like the United States, the communications center (if one can be identified) is not central. The whole point of the original plans that led to the Internet was to create a communications system without a center. When an information technology network is present, new forms of warfare need to be contemplated. It is society's dependence on and connection to the network that must become the focus. The same holds for other societal resources. Planning to disrupt or to defend against the disruption of the delivery of energy from a centralized power grid system or the support of financial transactions from a centralized banking system varies according to the degree to which such systems are networked.

The conceptual usefulness of netwar is clearest when one recognizes that new forms of human organization necessitate new thinking about conflict. As society becomes more networked, new vulnerabilities and new strengths will emerge. Analyzing the ways such weaknesses and strengths can be exploited for national security purposes will fall within the domain of netwar strategy.

Cyberwar

The increasing presence of the network form across society means that societal connectivity will begin to emerge as an important national asset itself. This will hold true for the networked military as well. The effects of information technology and the network form on the particular institution of the military means that, on the traditional battlefield, military connectivity will be of great significance.

Building on Arquilla and Ronfeldt again, I would refine the term cyberwar to refer to *conducting and preparing to conduct military operations against or in defense of military connectivity*. This reconceptualization broadens the term cyberwar beyond the narrow focus on command and control warfare. As the military organization becomes less centralized and hierarchical and more networked, it will be the overall flow and quality of information and knowledge that must be contested, rather than the specific control over information.

Netwar, Cyberwar, and the Strategy of Deterrence

How is the strategic dynamic of deterrence affected by a shift in focus toward connectivity? How do cyberwar and netwar affect the pursuit of deterrence, and to what degree are threats to connectivity contestable? Deterrence is best conceived as a game of strategy, where a move by one side shapes the response by the opponent.[10] The challenger seeks to produce as much freedom of action as possible by devising technical, tactical, and operational innovations that reduce (ideally to zero) the prospective costs of actions against an opponent. The deterring state or organization focuses on confounding the challenger's search for acceptable alternatives by developing a comprehensive response that approaches a guarantee of inflicting unacceptable costs on any state or organization that initiates an offensive challenge.

This competitive quest for strategic advantage between challenger and deterrer is referred to elsewhere as the strategic dynamic.[11] It is the heart of a deterrence environment. The dynamic itself revolves around two important theoretical concepts: shared information and rationality.

Shared Information

In order for deterrence to function, both the challenger and the deterrer must possess specific knowledge about each other's:

- national objectives
- commitment to the issue in dispute
- military, political, and economic resources available to support such a commitment and set of national objectives[12]

Incomplete or incorrect information about the challenger can lead to an insufficient deterrent, which promises either costs that are not considered prohibitive by the challenger or costs that do not cover the entire spectrum of military options open to the challenger. Without clear information about the capabilities and tactics of an opponent, the deterrence strategy will be vulnerable to the availability of countermeasures--weapons, tactics, or operational strategy--possessed by the challenger.

Information concerning the deterrer's objectives and capabilities that is shared with the challenger is critical. While a formidable range of retaliatory costs can be identified, deterrence will depend on the proper communication of those potential costs to the challenger. The fundamental problem associated with this requirement of shared information is the environment in which it must take place. A challenging state motivated to the point of actively planning the use of force is unlikely to be receptive to threatening messages from the opposing side. The deterring state will have to provide information to resolve two general questions dominant in the challenger's decisionmaking process: Does the deterrer possess the political determination and ability to follow through on the deterrent threat? And, does the military capability to inflict the threatened cost exist?

Rationality

Deterrence can fail for two reasons: the deterrer's strategy does not raise costs above expected benefits to be gained by military action; or, the deterrer's strategy threatens sufficient costs, but the challenger miscalculates.

Assuming that a country is not basing its deterrence strategy on bluff, a deterrent threat should encourage a challenger to calculate rationally all possible options. The deterrer should want a potential challenger to assess deterrent threats in an intelligent and consistent fashion. A properly designed deterrence strategy will cause the challenger to calculate that the expected benefits of the use of force will be negated by the costs inflicted by the deterrer's response. The problem, of course, is that the deterrence environment is not especially conducive to rational decisionmaking.

Effective rational decisionmaking is threatened by the conditions brought on by immediate deterrence situations. Both deterrer and challenger must manage decisionmaking in an environment of heightened tension, perceived time constraints, and ultimately stress, all of which can degrade rational decisionmaking.

Since a decisionmaker's susceptibility to stress, rationalization, or other factors is partly a function of constraints on time, the challenger should be persuaded that a strategy of delay would be more beneficial than one of hasty action under the limits of incomplete information evaluation.[13] The other conditioning factor that may lead to irrational decisionmaking is uncertainty. The potential for misperception (and its attendant promotion of irrational decisionmaking) increases under the condition of uncertainty. To promote a decisionmaking process that will lead the challenger to evaluate rationally the consequences of deterrent threats in a way that matches the expectations of the deterrer, uncertainty needs to be reduced. A challenger must be made aware that the deterrent threat, when employed, will inflict severe and specific costs.

Although pure certainty cannot be achieved, deterrence strategies can promote greater or lesser degrees of certainty. The development of an unambiguous deterrent force structure that can, when employed in retaliation, inflict the costs that were threatened is essential for mitigating uncertainty and thus encouraging a rational preference to yield on the part of the challenger. Coming full circle in our deterrence logic, the reduction of uncertainty for the enhancement of rationality is inextricably tied to the requirement and problems of shared information.

The intensity of the strategic dynamic associated with deterrence environments is greatly affected by the types of weapons that support deterrent threats. Nuclear deterrent threats have a degree of "reliability of effect" that makes the costs associated with a nuclear response seem incontestable.[14] Traditional conventional weapons, however, are susceptible to technical, tactical, and operational manipulation to a significant degree. The costs associated with conventional deterrent threats are generally viewed by opponents as contestable. The strategic dynamic is thus muted in the nuclear deterrence environment and exacerbated in a conventional one, making attempts to deter in the latter difficult over time. The more contestable that deterrent costs appear to be, the more susceptible they are to challenge.

Netwar and cyberwar should be understood as the two general forms of combat that may fall under the heading of information warfare. Employing connectivity as their organizing principle, both forms can capture a variety of offensive and defensive strategies now being highlighted by security studies analysts and the Pentagon. Strategies are being developed for conducting operations across command and control, electronic, intelligence-based, psychological, economic information, and computer system spectrums.[15] Information warfare also has been discussed in the context of the pursuit of a strategy of deterrence. This linkage was spawned by two coinciding events--the Persian Gulf Conflict of 1990-91 and the end of the Cold War. The aftermath of both of these contests brought a renewed focus on conventional weapons and their ability to provide a deterrence umbrella over extended US vital interests.

In assessing deterrence capabilities, generally it has been argued that nuclear deterrence, particularly its extended form, was practiced in order to counter the nuclear arsenal and conventional superiority (at least numerical) of the Soviet Union. Remove such an adversary and the threat the United States is likely to face will be from smaller conventional forces that may or may not have the capability to use weapons of mass destruction (WMD). The Persian Gulf conflict revealed how advanced the United States was in high-tech conventional warfare, defeating on the ground in one hundred hours--with few friendly casualties--what at the time was considered the fourth largest land army in the world.

It is both natural and logical to emphasize as the cornerstone for national strategy those weapons and forms of warfare in which one dominates. For the United States in the mid-1990s, emphasizing extended conventional deterrence rather than nuclear deterrence has the added advantage of lending moral support to the pursuit of nuclear nonproliferation policies. By reducing reliance on such weapons the United States can argue more persuasively for others to do the same--or to forego the option altogether. Dr. William Perry, before becoming US Secretary of Defense, concluded that the success of high-tech weaponry and information-processing systems in Operation Desert Storm showed that this type of force, while

> certainly not as powerful as nuclear weapons . . . is a more credible deterrent, particularly in regional conflicts vital to US national interests. . . . The United States can now be confident that the defeat of a conventional armored assault in those regions could be achieved by conventional military forces.[16]

The Persian Gulf conflict certainly revealed the great effect that improved precision-guided weaponry informed by better intelligence and battle damage assessment (BDA) can have on the conventional battlefield. Both intelligence and BDA act as "force multipliers"; that is, they enhance the destructive potential of conventional weapons and in doing so present a challenger with a formidable threat. But as high-tech innovations begin to translate into organizational and doctrinal changes, how will the ability to practice deterrence be affected?

Deterrence and Cyberwar

Much of this article has been concerned with developing some definitional rigor around the variety of issues and terms associated with early discussions of information warfare. When analyzing deterrence dynamics, care must be taken to denote clearly the strategic conditions one is assuming. Cyberwar, the preparation and conduct of military operations against military connectivity, represents an enhanced dimension of conflict. On the one hand, it refocuses combat into a new area. As former US Army Chief of Staff General Gordon Sullivan explains it in reference to the abstract organizational chart, instead of focusing primarily on the boxes, as armies traditionally did, the 21st-century Army will direct attention toward the lines that connect those boxes. Connectivity is the key. Under this strategic notion, however, the application of deterrence strategy will have to contend with the type of dynamic associated with traditional conventional weapons; deterrence strategy will have to overcome the problem of *contestability*.

A menace to the connectivity of an opposing military may represent a significant threat, particularly if that military is highly dependent on those connections. Two related problems, however, present themselves. First, the disruption to the military network would have to be substantial for it to be feared. Destruction of only a segment of the network would not necessarily preclude the rest of the military force from achieving its offensive goals, and thus the deterrent threat directed toward connectivity would not likely be seen as prohibitive. Second, if one of the major objectives of moving toward a networked military is to provide it with greater sustainability through redundancy and economy of force, the deterrent threat directed at connectivity may suffer from a perceived low reliability of effect. If a state can hope to sustain attacks on its connectivity, it will likely view deterrent threats directed at connectivity as contestable and, in the moment of decision, of questionable credibility (in terms of the capability to inflict unacceptable costs).

If cyberwar is to be dominated by a contest for supremacy over the electromagnetic spectrum,[17] the side that achieves such supremacy will have an enhanced ability to see, decide, and move at a pace that should overwhelm adversaries. This spectrum of conflict is better understood in the context of offense and defense than deterrence. Since the operations of networked militaries will be dependent on their connectivity, combat will, by necessity, involve direct attacks on that connectivity.

The potential advantage of greater military connectivity is greater lethality. This is brought about on one level by having a better idea of where your opponent is and the capability to hit him precisely before he moves. The digital battlefield, with its shared situational awareness, promises to solve the traditional problem that "operational mobility has never matched the capability of intelligence to tell us what the enemy is trying to do."[18] In the days in which the horse was the primary source of transportation, intelligence moved at about the same speed as the enemy. The digital battlefield, by creating theater-level integrated sensor-to-shooter (TLISTS) capability, has the potential to allow detection and reaction that can outmatch the enemy's ability to move.[19] This force-multiplier effect is further amplified when one considers the value-added dimensions of the networked military.

Traditionally, the securing of flanks or reserves and general force protection required the deployment of combat troops. However, if the electromagnetic spectrum can be seized and "topsight" over the entire battlespace provided, combat troops would not have to be dedicated to protect flanks and rear areas not under potential pressure from the enemy.[20] Some of these combat forces could then be used in offensive operations. Thus, connectivity not only can create greater lethality, it has the potential to increase the number of combat forces available to commanders.

A force with such capabilities, provided and sustained by connectivity, should cause most opponents to take pause. States that acquire dominance in cyberwarfare could make the whole prospect of challenging them seem prohibitively costly. The problem, of course, is that such dominance can be contested, both before and after war begins. Command, control, communications, computer, and intelligence (C4I) assets are susceptible to disruption and failure. The employment of computer viruses, electronic disinformation, or direct destruction of sensing equipment could therefore become increasingly prevalent as the importance of connectivity increases. As the *Gulf War AirPower Summary Report* suggested,

> The more sophisticated and expensive the information gathering system, the greater the premium opponents will put on disabling it. . . . The pay-off for shooting down a state-of-the-art radar surveillance aircraft, for example, will surely attract efforts to do so.[21]

Cyberwar cannot be understood in a static context. The Persian Gulf conflict, considered by some a harbinger of cyberwar, may be a poor touchstone. In the future, opponents of high-tech networked militaries are unlikely to make the same mistake Iraq did by giving the United States a "free ride" to deploy and use its communications network.[22] This, of course, does not mean that the ability to overwhelm potential adversaries in cyberwarfare should not be used to promote deterrence against attacks on vital interests. It should be recognized, however, that cyber-deterrence suffers from the same inherent difficulties that are built into conventional deterrence. As long as the costs associated with a deterrent threat can be viewed by an opponent as contestable to a significant degree, deterrence is unlikely to hold under great stress. The dynamics associated with cyberwar would seem to support the conclusion that much more time should be directed toward the development of both offensive and defensive cyberwarfare capabilities, tactics, and strategies, than on deterrence models.

Deterrence and Netwar

The discussion to this point suggests that cyberwarfare differs little from traditional conventional warfare in developing deterrence strategies. Both forms of conflict are dominated by a strategic dynamic driven by the presence of contestable deterrent costs. Deterrence is, therefore, fluid, in constant need of maintenance, and in the end prone to occasional breakdown.[23] When applied to the concept of netwar, the utility of a deterrence model and the practicality of a deterrence strategy seem even more limited. Netwar focuses attention on societal connectivity, which can be attacked, disrupted, or destroyed on three different levels: the personal, the institutional, and the national.[24]

Societal connectivity can be disrupted by targeting the electronic records of individuals. By changing or destroying the records that define a digital persona, one can alter whom society thinks an individual is and how an individual interacts with others. These records include credit reports, medical histories, school transcripts, financial portfolios, and bank accounts, as well as social security and law enforcement files. Manipulation of these records could effectively change one's wealth or even one's identity.[25] The seriousness of this threat (it is not simply a potential nuisance) is compounded by the general public's view of computer information. As Winn Schwartau emphasizes, the perception is that "computers don't lie . . . . In cyberspace, you are guilty until proven innocent."[26] Anyone who has ever attempted to challenge his or her credit rating report or deal with a government agency like the Department of Motor Vehicles can attest to this observation. Computer printouts are perceived as truth. You must prove the computer wrong. In most instances, the difference between the reality the computer describes and the one to which you attest can be explained away by a data entry error. But if manipulation of the digital record were to occur on a large scale and in a sophisticated and purposeful manner, the social disruption could be astounding.

Again it is important to recall the nature of the Information Age. The accessibility, availability, affordability, and speed of information management and the likelihood that all of these things will continue on their current trends create the potential for many significant advances. The nature of connectivity, however, breeds some serious potential second-level vulnerabilities as well, to the degree that electronic privacy begins to sound like an oxymoron.

The information dependencies and foundations of societal institutions are equally vulnerable. Take the modern corporation, for example. As the financial strength of the corporation becomes increasingly tied to its ability to manage information more effectively than its competitors, information systems may become new arenas for economic conflict. Rather than "send the fleet" to open and manipulate markets, competitors (be they territorial states, other corporations, or disillusioned former employees) may prefer to place at risk network systems supporting economic activity in the targeted industry, state, or region. Why compete in expensive marketing contests, when disruption of R&D projects before production even begins might be possible with a well-placed computer virus?[27] Instability in major corporations could have wide-ranging adverse effects on a society in general.

The consequences of netwar--disruption or destruction of societal connectivity--need not be limited to specific attacks on personal electronic or institutional records. It may be conducted on a broader scale, where electronic connectivity is indiscriminately targeted. At its core the high-tech network relies on electronic circuitry that is extremely vulnerable to disruption by other magnetic fields. We have all experienced some form of "interference," as when one's conversation on a portable phone is cut out by static created in passing by something as benign as an audio baby monitor set up in the kitchen. Such interruptions tend to be temporary. But little technical expertise is needed to manufacture enough of a magnetic field in a directed fashion so as to put at risk the circuitry of an individual computer or computer system. Weapons such as HERF (high energy radio frequency) guns and EMP/T (electromagnetic pulse transformer) bombs are not only conceivable but may already have been built.[28] The use of such weapons to disrupt an entire city's transportation, communication, or financial transaction systems begins to blend into cyberwar, where political-military command and control may be also affected. In a strict use of our term, however, such disruption would be a side effect.

The three levels of netwar do not fit well into a deterrence model. At its core, deterrence theory rests on the principle of retaliation in kind, where the cost inflicted in retaliation will at least match the level of costs associated with the offensive attack. If an attack reduces no buildings to rubble and kills no one directly, but destroys information, what is the response? We tend to think about information as intangible, but the *loss* of information can have tangible personal, institutional, and societal costs. What credibly can be placed at risk that would dissuade a state contemplating such an

attack?

The quick answer is, of course, their connectivity, but there are at least three problems with this answer. First, it presumes that the attacking state depends on and values societal connectivity as much as the deterring state. The Information Age, however, allows access to information warfare capabilities (both cyberwar and netwar) to anyone, not exclusively to those in high-tech networked societies. The United States may have required an advanced technological infrastructure to produce the global positioning satellite system (which it exploited to great effect during the Persian Gulf war), yet one can now go to Radio Shack and purchase a GPS monitor to access the system.[29] Information Age technology is inherently accessible, and one cannot presume the loss of connectivity will be viewed as prohibitive for a low-tech society. The question, then, is whether you threaten physical destruction of national assets in response. In essence, do you treat attacks on societal connectivity as acts of conventional war?

The second problem with retaliating against connectivity is its potential adverse effects on the deterrer. Connectivity has so far been treated as if it were a nationally bounded asset. But the nature of high-tech networks is that they challenge the usefulness of geographical boundaries as the unit of analysis. The connectivity of a "nationally" defined networked society does not respect geographic conventions. It is difficult to separate out disruptions in connectivity between national and global levels. This sort of electronic interdependence should in theory work to create disincentives against offensive attacks in the first place, but here again, subjective estimates of value may make a difference.

The third and most significant problem of a deterrence strategy based on "retaliation in kind" is that the attack may not emanate from a state at all. The technology is such that small groups--terrorists, organized crime, hackers--now have a capability that once belonged only to states themselves: in their anonymity they can nonetheless threaten instant societal-wide damage. Deterrence requires that the opponent be identifiable, which may not be the case in netwar. Consequently, general defense against attacks would seem to take on greater importance than developing credible deterrent responses. Of course one can threaten to seek out "netwarriors" and promise great retribution, but there is a lot of room between threatening them and finding them.

Once again, contestability as an analytical concept may prove helpful. The ultimate way to contest a promise of retaliatory costs is not to be identified as the source of an attack. The prospect of avoiding detection in netwar is at least high enough that most actors sufficiently motivated to contemplate such warfare will be unfazed by promises of future discovery. It may be prudent from a deterrence perspective to consider netwar as being no different from a traditional military attack on one's homeland and thus be ready to threaten an appropriate military response. However, the degree of ambiguity that is likely to revolve around this new form of conflict will undermine the credibility of such an approach in the eyes of a motivated actor.

Conclusion

The nuclear context of the Cold War raised deterrence to the dominant position of strategic thought. Great-power conflict was something to be avoided, not fought and won. For the Cold War superpower competition, deterrence was the primary strategic approach under which offensive and defensive structures provided support. The enormity of the potential destruction associated with nuclear weapons required such a focus. This, in turn, led to the extension of the deterrence concept to help organize thinking about the protection of extended vital interests and homelands through reliance on conventional weapons, an extension of the concept of deterrence that generally misses the significant difference between nuclear and conventional deterrence.

Traditionally, however, a state has been able to avoid being the object of attack through the development of an imposing offensive capability and a formidable ability to defend. In such a context, offense and defense dominate strategic discourse, and deterrence is best viewed as a by-product. The nature of netwar and cyberwar lend themselves to analytical frameworks and a strategic calculus dominated by offense-defense models, rather than by deterrence. The high degree of contestability likely to be found in netwarfare and cyberwarfare operations means that net- or cyber-deterrence will best be pursued as by-products of robust offensive and defensive strategies. Attempts to simply roll information warfare into strategic approaches in which deterrence is the primary concern miss what is distinctive about this new form of conflict--the contestability of connectivity. As we move closer to the 21st century, ironically, it is the

approach to war that dominated the early part of the 20th century (offense-defense) rather than its latter half (deterrence) that may be most useful for understanding information warfare.

NOTES

1. Vice Admiral Arthur Cebrowski, Director for Command, Control, Communications, and Computers for the US Joint Staff is quoted as saying that the services have yet to agree on what information warfare encompasses, but argues that since "the implications are so new, it is best that no central authority control its development." Quoted in Patrick Cooper, "Information Warfare Sparks Security Affairs Revolution," *Defense News*, 12-18 June 1995, p. 1.

2. Cited in Wayne Rowe, *Information Warfare: A Primer for Navy Personnel* (Newport, R.I.: Naval War College Center for Naval Warfare Studies, June 1995), p. 3.

3. John Arquilla and David Ronfeldt, "Cyberwar is Coming!" *Comparative Strategy*, 12 (Spring 1993), point to the Mongols as a perfect example of a military force that exploited information superiority. A similar point is made in Norman Davis, "An Information-based Revolution in Military Affairs," *Strategic Review*, 24 (Winter 1996), 43-53.

4. Martin C. Libicki, "What is Information Warfare?" *Strategic Forum*, No. 28 (Washington: National Defense Univ., Institute for National Strategic Studies, May 1995).

5. Martin Libicki and John Arquilla to date are the most often cited authors with regard to basic terminology, and both make this distinction.

6. Joseph E. Oder, "Digitizing the Battlefield: The Army's First Step to Force XXI," *Army*, 1 May 1994, p. 38.

7. Oder employs this term in much the same manner as I do when theorizing about the implications of the network form of organization, although he as well as William Perry focus on how this aids in combat effectiveness rather than on how this phenomenon might affect organizational structure and dynamics. See William Perry, "Desert Storm and Deterrence," *Foreign Affairs*, 70 (Fall 1991), 69.

8. Arquilla and Ronfeldt, pp. 144, 146-47. Rather than offer two new terms, I believe that debate is best forwarded by developing and improving upon existing terms.

9. Robert Anderson et al., *Universal Access to E-Mail: Feasibility and Social Implications* (Santa Monica, Calif.: RAND Center for Information Revolution Analyses, 1995), pp. 152-57. Specifically, they measured nodes. "A node may consist of a single computer and user or an entire organization with many of both. The Matrix Information Directory Service (MIDS) tracks and maintains historic data on the size of these networks aggregated by country. The `interconnectivity' metric used here is a combined measure of MIDS data on nodes per capita per country for each of the four major computer systems that can exchange electronic mail" (p. 156).

10. Thomas Schelling, *The Strategy of Conflict* (New York: Oxford Univ. Press, 1960).

11. Richard J. Harknett, "The Logic of Conventional Deterrence and the End of the Cold War," *Security Studies*, 4 (Autumn 1994), 86-114.

12. Jonathan Shimshoni, *Israel and Conventional Deterrence* (Ithaca, N.Y.: Cornell Univ. Press, 1988), pp. 10-16; Philip Green, *Deadly Logic: The Theory of Nuclear Deterrence* (Columbus: Ohio State Univ. Press, 1966), pp. 185-88.

13. Ole Holsti, *Crisis, Escalation, War* (Montreal: McGill-Queen's Univ. Press, 1972), p. 233.

14. I am indebted to Colin S. Gray for developing the phrase "reliability of effect" when he discusses my concept of contestable costs in Gray, "Nuclear Weapons and the Revolution in Information Warfare," in T. V. Paul, Richard J. Harknett and James J. Wirtz, eds., "The Absolute Weapon Revisited: Nuclear Arms and the Emerging International Order" (under review, 1996). For more on the incontestability of nuclear deterrents, see Harknett, "State Preferences,

Systemic Constraints, and the Absolute Weapon," in that same volume.

15. Libicki, "What is Information Warfare?" and Rowe, "A Primer for Navy Personnel," work with these terms. Interestingly, Libicki separates them into two broad categories--against society and against the military, which is the same distinction captured by my adaptation of netwar and cyberwar.

16. Perry, p. 66.

17. Morris Boyd and Michael Woodgerd, "Force XXI Operations," *Military Review*, 74 (November 1994), 16-28.

18. Arthur DeGroat and David Nelson, "Information and Combat Power on the Force XXI Battlefield," *Military Review*, 75 (November-December 1995), 58.

19. Randall Bowdish, "The Revolution in Military Affairs: The Sixth Generation, *Military Review*, 75 (November-December 1995), http://www-cgsc.army.mil/cgsc/milrev/95novdec/bow.htm.

20. David Gelernter develops the concept of topsight, which captures the essence of shared situational awareness. See his *Mirror Worlds*, p. 52; Arquilla and Ronfeldt also discuss the term in "Cyberwar is Coming!"

21. Eliot Cohen, "The Mystique of U.S. Airpower," *Foreign Affairs*, 73 (January-February 1994), 115.

22. William Perry acknowledges that "many of the C3I systems used in *Desert Storm* could be degraded by foreseeable countermeasures," p.79. Cohen makes a similar point, pp. 109-25.

23. Many conventional deterrence strategists assume that deterrence failure is ultimately necessary to strengthen deterrence. For an overview of this argument see Charles Allen, "Extended Conventional Deterrence: In from the Cold and Out of the Nuclear Fire?" *Washington Quarterly*, 17 (Summer 1994), 203-33.

24. This builds upon and modifies an argument put forward by Winn Schwartau, who discusses information warfare broadly defined as being conducted on the personal information, corporate information and global information levels. See his *Information Warfare: Chaos on the Electronic Superhighway* (New York: Thunder's Mouth Press, 1995).

25. On the vulnerabilities of automated teller machines, for example, see Paul Eng, "An Alarm Goes Off at the Cash Machine," *Business Week*, 31 May 1993, pp. 39-40.

26. Schwartau, p. 17.

27. For an overview of such potentialities, see Peter Denning, ed., *Computers Under Attack: Intruders, Worms, and Viruses*, NASA Ames Research Center (New York: Addison-Wesley, 1990).

28. For more on these weapons and their effects, see Schwartau, pp. 177-85. He refers to some early possible uses in the Gulf War as well as some instances in which the phenomenon of magnetic field disruption has disrupted or destroyed commercial and military systems.

29. See, for example, "Who Knows Where You Are? The Satellite Knows," *Business Week*, 10 February 1992, 120-21.

Dr. Richard J. Harknett is assistant professor of international relations in the Department of Political Science at the University of Cincinnati. He received his Ph.D. from Johns Hopkins University in 1991. He has published articles and book chapters on conventional deterrence theory, nuclear proliferation, and state territoriality. His current research includes a focus on security alignment theory. An edited volume, with T. V. Paul and James J. Wirtz, <169>The Absolute Weapon Revisited: Nuclear Weapons and the Emerging World Order,<170> is currently under review.

Reviewed 21 August 1996. Please send comments or corrections to carl_Parameters@conus.army.mil.