International Law Studies - Volume 76
Computer Network Attack and International Law
Michael N. Schmitt & Brian T. O'Donnell (Editors)

IV

Information Operations, Information Warfare, and Computer Network Attack

Their Relationship to National Security in the Information Age

Daniel T. Kuehl*

Introduction

What is "information warfare"? Is it nothing more than a bumper sticker, used as a "quick fix" rescue for budgets and programs that find it useful to attach themselves to the hot new concept? Is it such a revolutionary new amalgam of technologies and concepts that old and traditional forms of warfare are soon slated to fall into the same receptacle in which outmoded military technologies such as the catapult and war galley slumber? Is warfare as we understand it, featuring "blast, heat, and fragmentation," about to become obsolete?[1] The intent of this brief introduction to information warfare (IW) and information operations (IO) is to both explore these issues and present the thesis that they are best understood in light of the environment in which they take place—the information environment—and to explore the relationship of that environment to the specific topic on which this book is focused, computer network attack.

What is Information Warfare?

A useful starting place is to trace the evolution of the term information warfare itself. The earliest use of the term in the United States probably originated in the Office of Net Assessment, where in the 1970s Dr. Tom Rona was investigating the relationships among control systems, a field known as cybernetics. Dr. Rona described the competition between competing control systems as "information warfare," in the sense that control systems can be described as the means for gathering, processing, and disseminating information, processes which can be diagrammed and described with flow and feedback charts of mind-numbing dryness and complexity.[2] In 1993 the Department of Defense published an official definition for the term, in a highly classified DoD Directive, TS3600.1. There were actually several definitions, at differing levels of classification.[3] Not surprisingly, this definition was frequently revised as the operational and organizational implications of the concept evolved. The current definition has the record for longevity—more than five years at the time of this writing, since the promulgation of the current guidance on information warfare and information operations in DoD Directive 3600.1 on December 9, 1996.[4] The publication of Joint Publication 3-13, Joint Doctrine for Information Operations, in October 1998 probably ensures that the current official DoD definitions of IW and IO will remain in effect for some time longer.[5]

The present definitions leave much to be desired, however, if one is hoping to find explanations that clarify and explore what might constitute the character, conduct, and intent of IW and IO. But since one must understand what IO is in order to move to its less comprehensive building block, IW, these definitions do provide a useful starting point:

> Information Operations: Actions taken to affect adversary information and information systems while defending one's own information and information systems.

> Information Warfare: Information operations conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries.

There is actually a second sub-activity of IO that is critical to national security in the Information Age, namely information assurance (IA), defined thus:

> Information Assurance: Information operations that protect and defend information and information systems by ensuring their availability, integrity,

> authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.[6]

While these definitions throw a less-than-blinding light on their constituent activities, there is one critical theme that they are intended to bring out, and that involves "who" does them and "when" they are done. IW is clearly a military activity conducted under a special set of circumstances, whereas IA involves not only the military, but also government at all levels, and even portions of the private sector. Therefore, IO as an activity goes far beyond just the military during conflict, to include the government and a wider range of private sector activities than perhaps that sector or even the government recognizes.

Most US service concepts of IW rest in part on the concept of the "information environment." Whether described as an environment, realm, domain, or whatever, there is a clear sense that information has become some kind of "place" in which crucial operations are conducted. The Army's trailblazing 1996 doctrinal publication, Field Manual 100-6, Information Operations, even speaks of a "global information environment [and] battlespace" in which conflict is waged. The latest version of the USAF's basic doctrinal publication, Air Force Doctrine Document 1, published in 1997, explicitly addresses the need to dominate the information realm, and discusses information superiority as "the ability to collect, control, exploit, and defend information while denying an adversary the ability to do the same . . . [it] includes gaining control over the information realm. . . ."[7] Joint Pub 3-13 defines it somewhat differently as "[t]he capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same." Both, however, share the sense that information superiority involves doing something to the adversary while protecting ourselves in order to control and exploit the information environment. Using this philosophy, then, IW and IO can be described as the *struggle to control and exploit the information environment*, a struggle that extends across the conflict spectrum from "peace" to "war" and involves virtually all of the government's agencies and instruments of power.[8] One appeal of this approach is that if one replaces "information" with "aerospace" or "maritime," you have defined air and naval warfare, or more appropriate to our purposes, airpower and seapower. Information operations can thus be described as those activities that governments and military forces undertake to control and exploit the information environment via the use of the information component of national power.

This immediately raises another question: what is the information component of national power? More than just another bit of computer-age terminological fluff, its origins actually predate this decade, starting with the strategies developed by the Reagan Administration in its very real struggle with the former USSR. In 1984 the Reagan Administration issued National Security Decision Directive 130, US International Information Policy, which outlined a strategy for employing the use of information and information technology as strategic instruments for shaping fundamental political, economic, military, and cultural forces on a long-term basis to affect the global behavior of governments, supra-governmental organizations, and societies to support national security.[9] This is hardly a new concept, and clearly governments and leaders have been exploiting the information environment for centuries. Indeed, one could argue that the stone carvings that Assyrian rulers made of conquered peoples and cities being enslaved and pillaged were intended as much to cow and terrify current and potential subjects as to inform archeologists thousands of years later about what hard and cruel folks they were. Regardless of the fact that the information technology being employed was stone and chisel, and not microchip and computer network, this was exploitation of the information environment for strategic political objectives.

Two examples from this century will suffice to illustrate the critical importance of this environment to national security. The first took place on August 5, 1914, when the royal cableship *Telconia* sortied into the North Sea and severed all five of Germany's direct undersea telegraph links with the outside world. After that date, the view that the rest of the world had of The Great War increasingly passed through a lens located in London. This enabled British information warriors to mount a very effective strategic perception management campaign that eventually helped bring the United States into the war on the side of the Allies, thus moving from strict neutrality to waging war to "make the world safe for democracy." Great Britain was exploiting the information component of national power. The second example comes from the Cold War and the efforts by the United States and some of its allies to exploit another segment of the information environment—radio—to weaken the political cohesion of the Soviet Union and the peoples it controlled. Radio Free Europe did not by itself, of course, cause the fall of communism and the Soviet government, but it certainly had its role to play. It is perhaps instructive that certain elements within the former Soviet Union still blame Western IO for communism's collapse.[10] Yet since both these examples employed old information technologies—telegraph cables and radio—they also beg the question: what is the role of the computer in all of this?

A New Geostrategic Context

The previous examples raise the question of what is so new and different about the current state of the "information environment" to warrant all the fuss about "computer network attack" and information warfare. The answer is fourfold: cyberspace, digital convergence, global digital omni-linking, and computer control of infrastructures, all of which are synergistically combining to create a new geostrategic context for national security.

One's receptivity to the changes of the information revolution is often revealed by the reaction to the word "cyberspace." At the very utterance of the word, doubters and skeptics display intellectual and sometimes even physical discomfort, while the "digerati" and those at ease with the technologies of the information age react as if someone had said "traffic" or "radio" or any other commonplace term. Almost everyone is familiar with the use of information as a tool, a process, even a weapon—recall the earlier comment about "blast, heat, and fragmentation"—yet while all of these remain not only applicable but even vital to the new and evolving "American way of war," none in isolation goes far enough. This chapter argues that the synergistic effects of electronic digital technology, acting in and on societies that are becoming increasingly information-dependent, have made information into a virtual environment, with cyberspace as its physical manifestation. Cyberspace, defined here as that place where electronic systems such as computer networks, telecommunications systems, and devices that exert their influence through or in the electromagnetic spectrum connect and interact, has always existed, but not until mankind invented technologies that operated via the electromagnetic spectrum did it become "visible" and noticed.[11] A useful analogy is outer space. It has always been there, but not until humans developed technologies for extending our activities into it and used it to affect terrestrial affairs did we fully comprehend that it is another physical and operational environment in addition to the land, sea, and air. Outer space does not have the same physical presence or properties of land or water because you cannot "weigh" it or "measure" it in a useful sense, but it nonetheless exists because we can see the physical results of things that happen there.[12]

The physical laws and principles that govern and delineate how systems function in these environments are the borders that fix their boundaries.[13] Submarines, for example, function very well in an environment governed by the laws of hydrodynamics, but they cannot fly. Armored fighting vehicles function effectively on land, but they are useless in space. All of these distinct and unique environments synergistically interact with each other, and the same holds true for cyberspace. The devices and systems that operate in cyberspace—radios,

radars, microwaves, computer networks—function because they conform to and exploit the laws governing radiated and electronic energy. We can date our use of this environment to the mid-19th Century and the invention of the telegraph, which was the first telecommunication system to operate in accordance with the laws of this medium.[14] The following century saw regular and ever-more technologically sophisticated advances in our ability to control and exploit this medium—undersea telegraph cables, radio, television, microwave relay, even communications satellites—that extended the reach of telecommunications to continental and eventually intercontinental distances. We have increased the volume of information that we can store, manipulate, and transfer to previously unimaginable proportions, but it was only in the closing quarter of the 20th Century that the fortuitous, perhaps even serendipitous, marriage of these technologies with the microchip led to attainment of "critical mass" and the emergence of cyberspace as a full fledged environment in which military forces and society in general—politics, business, education, and more—began to learn how to operate. Given this definition of cyberspace, we see the link to computer network attack; cyberspace is the physical environment in which such operations take place.

Cyberspace is the basic arena in which two additional developments of the information revolution are transforming the strategic landscape: the increasing capability to transform almost any kind of information into ones and zeroes, in what is known as *digital convergence*, and the growing Internetting of global telecommunications media in a condition referred to here as *global omni-linking*. Although these developments are distinctly different, they are at the same time synergistic and interdependent. Thomas Kuhn suggested in his landmark study of scientific revolutions that the history of technological advancement has not been one of steady discoveries or developments, but rather one marked by spikes or sharp advances that flow from extraordinary finds or revelations that yield discontinuous and revolutionary changes.[15] Such has been the case with information technology. Advances in communication technologies prior to the middle of the 20th Century were relatively linear—telegraph to telephone to radio and so forth. The break point came with the invention of the microchip because the synergistic advances in information storage, manipulation, and transmission capabilities made possible by digital convergence are happening at an ever-increasing and nonlinear rate. These developments have occurred in two areas, the *speed* of information manipulation/transmission, and the *volume* of information that can be manipulated/transmitted. The combination of these attributes with computer-enhanced and controlled telecommunications systems have led to the "*omni-linking*" of the electronic digital world. In a word, the globe is now

"wired." The explosion that has resulted from the application of the microchip to communications technologies has formed the new science of telematics—the marriage of computers and telecommunications.

Telematics has created a new operational environment. The technology of the telematic age we use to exploit cyberspace is new, perhaps less than two decades old, and global omni-linking is inseparably tied to the emergence of cyberspace as an operational environment. While current technology is actually rudimentary compared with what the future holds in store—compare the level of aviation technology in the 1930s (biplanes) with what came just half a century later (747s and B-2s)—the omnilinking of the world is increasing every day, as more and more computer networks and telecommunications systems tie together and pass the lifeblood of today's economic and political world . . . digital information. The degree to which our societal dependence on this environment is growing is startling. Our military forces already depend on it. The Persian Gulf War of 1990-91 simply could not have been fought in the way we fought it without precision information for precision weapons, command and control systems that enabled us to operate like a matador around a woozy and half-conscious bull, or satellite communications links that enabled organizations half a world away (NORAD) to monitor Iraqi missile launches and pass targeting information to Patriot batteries to engage the missiles.[16] Our microchip-driven information collection, storage, manipulation, and transmission capabilities are so advanced, and the links that move the information around so Internetted, that we worry that TV news commentators on the east coast could skew election results on the west coast by announcing "analysis of voting trends indicate candidate 'Z' has won the election." The global economy cannot function without the constant supply of digital electronic information. It has become a form of energy or capital, and global business is utterly dependent on telematic systems and capabilities to keep the world's economy going twenty-four hours a day. Business practices such as "just in time inventory," or military techniques such as "just in time logistics," cannot function without the digital information that fuels it. In a very real sense, Joint Vision 2010,[17] which could be called the "new American way of war," is possible only if American forces possess "information superiority," defined by Joint Pub 3-13 as "[t]he capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same." The "Internet" is neither a finite place nor a collection of gadgets such as routers and switches; it is a description of the increasing omni-linking of the world. Thinking of the Internet in terms of its users, such as "America OnLine" or "CompuServe," or in terms of uses, such as chat rooms or E-commerce, is as shortsighted as describing

aerospace in terms of an airline. While some dismiss this environment and the Internet as merely entertainment or worse, this view ignores the fact that a very large percentage of the information currently available on TV or in print would fall into the same category. Few, however, would deny the impact of visual media on the American populace's support of the Vietnam War or the impact of the printed word on democracy and freedom via the "Declaration of Independence" or "Emancipation Proclamation." What is different is that the Internet and omni-linking make it increasingly possible for that televised image to be seen instantly by an ever increasing percentage of the world's population, or for that opinion-shaping paper to be sent to tens or even hundreds of millions of people simultaneously and in their own language.[18] Digital convergence, combined with connectivity, adds up to the second major part of the fundamental difference between the information age and the period "BMC"—"Before the Micro Chip."

The final major development shaping the new geostrategic context is the increasing reliance on computerized networks for the control and operation of key infrastructures in advanced societies. The growing reliance on these systems for the control and functioning of an increasingly large segment of the infrastructures on which we depend for economic, social, political, and even military strength is both a boon and vulnerability. As suggested by Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6510.1, Defensive Information Warfare, "use breeds dependence, and dependence creates vulnerability."[19] Whether it be the supply of energy (electricity, oil, gas), the management of transportation (railroads, air traffic control, motor vehicle movement), the transference of digital wealth (electronic funds transfer, digital banking, control of stock exchanges), or the operation of the very telematic media that supports the entire structure, look below the surface of almost any segment of daily life in modern societies and one will find Internetted and interlinked computer systems.[20]

The degree to which this is invisible to the general populace is illustrated by a real incident. In February 1996, Washington DC suffered a tragic but relatively typical industrial-age accident—a train wreck. During a snowstorm a commuter train collided with a freight train, and several people were killed. The investigations by the news media examined almost every aspect of the accident, including the signaling system that provided instructions to the train operator (who was also killed, heroically trying to warn passengers instead of saving himself) via the ubiquitous signal lights that line railroad tracks all over the world. The news media focused on whether the operator saw the signals, whether they were properly placed, or whether they functioned properly. None asked whether the signals

had been electronically tampered with (they had not been), nor even raised the issue of how the signals were controlled or where those controls were located. They were controlled, of course, by Internetted computer systems, and the computers which control the rail signals for the trackage in Washington DC are located at the operations center for CSX Railways, in Jacksonville, Florida, several hundred miles distant. This is an illustration of how deeply imbedded within modern societies such control systems have become, and how unaware most of us are of their functioning.[21]

It is a government responsibility, however, to not only be aware of such developments, but also to take precautionary and preventive measures to mitigate potential disruptions to the effective functioning of systems upon which the society and national security depend. In July 1996, the Clinton Administration issued Executive Order 13010, which directed the formation of a unique commission, the President's Commission on Critical Infrastructure Protection, or PCCIP, which brought together senior governmental officials and representatives from those private sector industries and businesses that comprised these key infrastructures into a commission tasked with studying the vulnerability of these infrastructures to disruption. While the commission examined both the physical and cyber threats, they freely acknowledged that their emphasis was on the cyber threat, in part because it was—and remains—less well understood than physical threats. Their conclusion that the threat is real and growing might seem unsurprising and perhaps even preordained, but nonetheless reflects the growing awareness that our very dependency on computerized control of infrastructures creates an inherent vulnerability that is at the heart of hypothetical scenarios for information warfare in which computer network attacks on critical infrastructures "take down" key segments of those infrastructures and thus generate cascading effects on such systems as transportation, banking, or emergency services. It was the need to respond to this vulnerability that caused the Clinton Administration to issue Presidential Decision Directive (PDD) 63 on May 22, 1998, establishing a national coordinator for infrastructure protection within the National Security Council and creating an organizational structure by which such threats and vulnerabilities could be mitigated. PDD 63 called for a public sector-private sector partnership to develop cooperative procedures and organizations to assess the threats and vulnerabilities and create countermeasures, and thus stands as a landmark step in what is now called computer network defense (CND) against the threat of what has in some quarters been termed "infrastructural warfare" employing computer network attack (CNA).[22] But as perhaps the key element in information warfare, is the computer network the target, or merely the means to the target?

Computer Networks, National Security, and the "Metanetwork"

This chapter has already used several terms relating to computer networks without defining those activities. The current CJCSI 3210.1, Joint Information Operations Policy, dated November 6, 1998, currently includes three such activities, defined thus:

> Computer Network Attack (CNA): Operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves.
>
> Computer Network Defense (CND): Measures taken to protect and defend information, computers, and networks from disruption, denial, degradation, or destruction.
>
> Computer Network Exploitation (CNE): Intelligence collection operations that obtain information resident in files of threat automated information systems (AIS) and gain information about potential vulnerabilities, or access critical information resident within foreign AIS that could be used to the benefit of friendly operations.[23]

The thread that ties these activities together is the computer network. The network may be the actual target, in the sense that the attacker wishes to make the network cease its function of transferring information. It may be the means to affect another target, such as a database or other information-based process, in which the attacker does not want to cut the network, but rather use it in order to impact or degrade an adversary's decision-making process. The objective of computer network defense is to prevent an adversary from doing either of these to our networks. Computer network exploitation is specifically concerned with intelligence operations. While the dividing line between CNA and CNE may well be very murky—indeed, a single keystroke might be the only difference—we will not discuss CNE or even CND further, in part because those operations bring along their own baggage train of thorny issues and unresolved questions. CNA will be a sufficiently difficult problem to address here.

Imagine for a moment that a warrior (the specific service or warform is irrelevant) has just destroyed a critical target, comprised of all the computerized databases contained in the enemy's central C3 facility. Does it matter if this was done with a laser-guided aerial bomb, a five-inch round from a warship at sea, a

120mm round from a tank, a ballistic weapon dropped from space, or via malicious programming code "delivered" by computer intrusion? The definition of CNA cited above does not clearly state the answer, but it is this author's contention that the means used is immaterial; since the intent clearly conforms to the spirit of the definition, any or all of the examples just cited could be CNA. In all but the last case, however, warriors and jurists alike probably consider themselves to be on fairly firm ground. It is the last case that gives everyone pause. In part, this comes from our intellectual and doctrinal desire for clarity. Warriors seek to clearly distinguish between different kinds of operations so that they can establish clear lines of authority and control. Unfortunately, this may not be fully possible in the information battlespace. The example cited above could be air, naval, land, or space warfare, in addition to being information warfare. This is not unique to information warfare, although we do not often examine military operations from such a multi-doctrinal perspective. During the October 1973 Yom Kippur War, for example, once Israeli armored forces crossed the Suez Canal in their counteroffensive they began destroying Egyptian surface-to-air missile forces, which enabled the Israeli Air Force to expand operations. This is a wonderful example of what airmen term Suppression of Enemy Air Defenses, or SEAD. Doctrinally, SEAD is a part of what is in turn called Counterair Operations—things done to seize and maintain control of the air. Thus, armored forces were part of an air superiority operation at the same time they were engaging in what ground forces would call maneuver warfare. This same kind of doctrinal flexibility must also be applied to information warfare and CNA.

The first aspect of CNA mentioned above focused on the destruction or negation of a network. Regardless of whether this is accomplished kinetically—the laser guided bomb, for example—or via cyberspace, the intent remains the same, to prevent the adversary's use of the network. We will not consider kinetic means further, since they are already well understood, but the use of the computer to negate another computer is less well understood. There is no need here to discuss the intricacies and details of computer code, and such issues are addressed in great detail in a myriad of books on computer security and information technology. That said, a word or two on the basic context are in order.[24] The basic objective of virtually any computer intruder or hacker is to be able to operate within the system as if he/she owned it. Once this level of access is gained, the pseudo-owner can then change programs, functions, addresses, and almost any other aspect of the way the computer or the entire network in which it resides operates. Thus, an intruder that obtains root access into a computer network that controls personnel records, for example, could perhaps alter the content of those records or change how those records are stored or transferred.

The implications of this for the proper functioning of any computer network, be it military, government, or business, are obvious.

As pointed out earlier, modern technologically advanced societies are increasingly dependent on computer networks for a growing range of societal and national security needs. If the computer system that controls rail operations in the southeast United States can be degraded, for example, it will slow down or perhaps even stop the movement of military forces that depend on rail links to move to their deployment locations. If the telephone system that supports Scott Air Force Base, headquarters of US Transportation Command, Air Mobility Command, and the Tanker-Airlift Coordination Center, can be severely degraded it could seriously hinder the movement of US forces overseas. If the energy management system (electric, gas, and oil) in the northeast could be degraded during severe winter weather it might cause a refocusing of national political and strategic attention away from a distant and perhaps poorly-understood overseas problem to an unfolding disaster right at home. Some of the discussion of infrastructural vulnerability seen recently has given far too little credit to the resiliency and robustness of these networks. However, while loose talk of "taking down" entire national infrastructures is fanciful at best, it also remains true that all of these infrastructures are in some degree vulnerable to intrusion and degradation. Examples as recent as the 1999 Kosovo conflict, during which a variety of allied computer networks such as the NATO e-mail system came under attack via what was a "denial of service" effort to overload the system with electronic traffic, indicate that this will be an active battlespace in the future.[25]

If the intent of a CNA is to partially or completely deny access to or use of the network, defenders are faced with a thorny set of problems, but at least they will probably be aware that the system has been targeted. When you receive multiple thousands of unanticipated e-mail messages within a short span of time in what is termed a "spam" or denial of service attack, you can reasonably assume that someone—even though you might not know whom—means you harm. CNA that does not attempt to overtly prevent use of the system, however, but rather is intended to covertly subvert its purpose by changing the content, is perhaps an even more difficult problem. Let us use the analogy of a pipeline that is carrying jet fuel. In traditional, kinetic warfare, we would target it for destruction from the air, and a smart airplane carrying PGMs would come along and neatly blow the thing apart, thus preventing the enemy from refueling his jets from it. But what if we did not want to be so noisy? We could send a special operations unit to the pipeline, attach to it a small pumping device that injects a small but fatal (from a jet fuel standpoint, at least) amount of some nasty foreign substance, and, even though the pipeline itself is still intact, render the stuff flowing through the

pipeline unusable. It is a perfect analogy for digital modification of data, and it might be virtually invisible until too late. Let us assume that the computer code for "bomb, 500 pound" is a combination of forty-four ones and zeros, while the code for "bomb, 4,000 pound" is another combination of forty-four ones and zeroes—almost, but not quite, identical. The opportunity for logistical chaos is immediately apparent. If one eighth the anticipated number of munitions show up at Base X, but all of them are too large for the aircraft at that base to carry, some significant friction has just been injected into the air war. We have a long history of instances where accidental but incorrect computer code in systems that deal with telecommunications or energy has caused significant malfunctions with those systems, and we have seen a growing number of cases of intentional intrusion into these and other such computer networks.[26]

The mindset of many senior strategic leaders regarding the computer still seems to be that they are large, expensive, and stand alone in their respective "data center" somewhere. The reality is just the opposite—for they are small (and getting smaller every week), cheap (and getting cheaper every week), and interconnected on a global scale. It can be a difficult realization that if you operate a computer that is plugged into a telephone, you are theoretically connected to every other computer on the face of the earth that is also connected to a telephone, even if it is a cell phone—hence the strategic importance of what this chapter calls "omni-linking," because the globe is literally covered with countless individual computer networks that are nonetheless all part of the growing global "metanetwork" to which tens of millions of individuals, organizations, and entire societies are connected. It would seem to be inescapable that as more and more human activity is conducted in cyberspace via the metanetwork, it will become a battlespace and an arena for conflict. But will it be war?

Information Warfare—Is it "War"?

Perhaps a necessary starting point for this question is: what is war? Most members of the military and the national security community would have no difficulty recognizing Clausewitz's characterization of war as "an act of [physical] force . . . a pulsation of violence."[27] Too often, perhaps, the rest of the phrase, "to impose our will," is forgotten. The reason for the force and violence is the imposition of the will of one political entity onto another political entity. The issue at hand now is the potential ability of political actors to impose their will through informational means.

In the Clausewitzian paradigm, war was waged by a special class of actors, "warriors," on behalf of a special kind of political entity, "States." The warriors

were the uniformed military—soldiers, sailors, later airmen—and the States were the legitimate and recognized holders of international legal authority to engage in the force and violence of warfare. Almost at the same time (late 19th Century) as the Clausewitzian paradigm began rising to international prominence another force arrived on the scene, the international codification of legal norms for the conduct of war and the protection of certain classes of society. These norms, first enacted a century ago (1899) at The Hague, almost immediately encountered two extremely powerful forces: the nature of the modern industrial State and the influence of new technological means of warfighting.

The modern industrial State possessed an unprecedented amount of killing and dying power. Although this was clearly hinted at by the course of the American Civil War, the great European military powers failed to recognize it until too late.[28] The result was the stalemate and slaughter of The Great War and the Western Front, in which the amount of destructive force that the industrial State could generate was matched only by the amount of destructive force it could withstand. Twenty years later these same great powers demonstrated that their killing/dying power had actually increased, with the result that World War II's toll far exceeded that of World War I. This was made possible by the State's ability to employ and draw upon power sources that cut across almost the full breadth of society. These sources crossed the boundaries of what had been intended as sanctuaries and protected groups, such as undefended towns or noncombatants such as women. But did the concept of an undefended town mean anything useful in an era of nationwide air defense systems with flak belts and fighter patrols? Was "Rosie the Riveter" a protected person when she and her sisters left their homes to build U-boats or liberty ships?[29] It became increasingly obvious that the modern industrial State was a series of networks or infrastructures, and the American doctrine for strategic airpower in World War II was based on exploiting this fact. The "industrial web" theory of targeting, developed at the Air Corps Tactical School in the 1930s, came from precisely this paradigm and was based on the belief that if the critical nodes or "centers of gravity" (a 1990s adaptation of a Clausewitzian term) of an industrial State could be negated, the resulting stresses on the entire system would cause it to unravel like a spider's web whose critical connecting points have been cut.[30] The result of the interplay of these factors was a change in our paradigm of warfare, from the "limited" dynastic wars of the 19th Century to the "total" wars of survival—political, religious, racial, ideological—of the 20th Century.

A second critical factor was the development of new forms of warfare based on the exploitation of new forms of technology. The first great revolution in military affairs (RMA) of the last century was the adaptation of the internal

combustion engine to warfare, and by the end of the century's second decade warfare had become incredibly more complex than it had been in 1900 because it was now multidimensional. No longer was warfare waged on the surface. Now it went on below the ocean's surface and above both the sea and the land, and military success became increasingly dependent on the successful coordination of operations in all three dimensions. Thus, the invention and employment of the submarine and the airplane transformed warfare, a fact that was clearly visible during World War II in that no nation that failed to dominate all three environments was successful. To make the situation more complex, by 1945 it was clear that any force that was unable to operate in yet a 4th dimension—the electromagnetic spectrum, or what has here been defined as cyberspace—would have great difficulty operating successfully in any of the other three dimensions. This trend has continued and been intensified with military exploitation of yet another physical environment, outer space. The strategic and operational environment for warfare at the cusp of the new millennium now enfolds geospatial awareness, global connectivity, and a host of new factors that have further complicated the art of war. Not surprisingly, the legal context for conflict, which includes the law of war and the complex series of agreements and treaties that provide a framework for the affairs of State and conduct of statecraft, has been outpaced by the technologies available to global society. At the outset of the 20th Century, issues such as unrestricted submarine warfare and strategic bombing held promise of a disconnect between the law and war, while at its close other issues, such as netwar or the weaponization of space, hint at further uncertainty in how States and societies will attempt to regulate conflict. The same two forces that arose at the opening of the last century are still at work, with the notable difference that instead of the industrial age it is the information age that is changing the paradigm.

In some ways, the impact of the information revolution on warfare is quite apparent, and the application of advanced information technologies to traditional military capabilities and weapon systems—what could be termed information "in war"—serves to make "blast, heat, and fragmentation" work more efficiently and effectively. Information used as a weapon, tool, or even target is nothing new, even though the new technologies vastly increase its impact as an enabling capability or force multiplier. Sending target photos via secure fax from intelligence organizations in the United States to air campaign planners in NATO, thus enabling the destruction shortly afterwards of key Serbian infrastructure nodes via precision guided munitions, is an example of this fact. This exponential power as an enabler is an important, even vital aspect of what the Air Force calls "information in war,"[31] a critical foundation for information warfare,

but it is not synonymous with it. Information warfare is a new warform that is evolving from the synergistic effects of several new and unique factors, all part and parcel of the information revolution.

This brings us back, however, to the entering question: is this "war"? Does this fit with the Clausewitzian paradigm of force and violence? If a State is able to degrade an adversary's military capability, damage its key infrastructures, and inject great disorder into political systems or economic affairs, all without the use of kinetic force and violence, might not the recipient of such effects argue that they had indeed been "attacked" and were thus "at war" with the inflictor? During a recent exercise conducted annually at the Air Force Wargaming Institute by students from all of the DoD's senior military colleges, the "red team" developed a war plan against "blue" that included information warfare attacks against such targets as the air traffic control system, financial centers, energy distribution network, and telecommunications infrastructure, with the intent of degrading and disrupting blue's political will and strategic capability. The red team's objective was to seriously undermine the ability and will of both blue and its allies to continue armed opposition to red's other operations. This exercise in information warfare—which the students named "Dangerous Opportunity"—might be seen as a mirror-imaging of American attitudes and mindsets, but it also reflects technological conditions and vulnerabilities that the information environment may make available in any future conflict. It also closely tracks with recent publications by some senior Chinese officers, who postulated precisely such operations in their concept for "Unrestricted Warfare."[32] But does this perspective reflect any sort of consensus on what IW and IO are?

Perspectives and Doctrines

Earlier it was pointed out that the terminology of IW and IO are still evolving; not surprisingly, so are the various operational and doctrinal concepts held by the different organizations involved in the IW/IO effort, both in the United States and globally. It is worth some time to briefly explore some of these doctrinal and operational concepts. In the American military much of the future direction for IW/IO will come from "Joint Vision 2010," published by the Joint Staff in 1996, amplified in 1997 by "Expanding Joint Vision 2010: Concept for Joint Warfare," and further amplified by "JV 2020" in the summer of 2000.[33] JV2010, as it is called, postulated several dynamic changes in the overall strategic environment and the emergence of new operational concepts. A key hypothesis of JV2010 is that dramatic changes in new information technologies will make attaining and maintaining information superiority a critical requirement.

Concepts such as Dominant Battlespace Awareness or Network Centric Warfare are based on the assumption that new information technologies will enable US forces to develop and exploit networks of sensors, decision-makers, and shooters that can operate far faster than their adversaries, and thus translate information superiority into actual combat power.[34]

If the technologies of the information revolution are creating an information-based RMA, it remains for the American military to bring this to fruition by creating organizations, doctrines, and operational concepts to exploit technological advantages, and turn them into actual military capability.[35] In 1998 the Joint Staff finally published Joint Publication 3-13, Joint Doctrine for Information Operations. Like any such publication, it represents what all of the various coordinating parties could agree on, including the four military services. It is not a visionary document with radical new operational concepts, but it does emphasize that IO is not a technical capability, but rather a coordinating strategy for operations in the information environment, and it makes three critical points. First, joint forces at all levels must organize to conduct IO, and every one of the combatant commands, such as European or Central Command, have created full-time planning cells for IO. Next, the IO planning process must begin long before operations begin; it is too late to begin planning just a few days before the operation's scheduled initiation. Finally, joint forces must train and exercise in an information-intensive environment and engage all of the applicable organizations, including perhaps private sector or combined-multinational entities.

All US services—Army, Navy, Marine Corps, and Air Force—have approached IW/IO somewhat differently, viewing them through their individual warfighting lenses. The Army was the first service to publish specific doctrine for IO, and Field Manual 100-6, published in 1996, contained eloquent language about the "global information environment [and] battlespace," as mentioned earlier. But the doctrine's perspective was clearly on the need to "integrate all aspects of information to support and enhance the elements of combat power," those being the rather traditional: infantry, armor, artillery, and, to a lesser extent, airpower delivered via rotary-winged helicopters. The Army has chartered an organization, the Land Information Warfare Activity (LIWA) at Fort Belvoir, Virginia, to develop both concepts and capabilities for IO, and LIWA personnel have been active in the Balkans for much of the 1990s, assisting Army IO efforts there. The Navy views IO as something that enables fleet operations and makes those operations more efficient and effective. The Navy's perspective on IO also reflects the expertise and experiences of several of its different "communities," with two in particular, space/electronic warfare and cryptology, as having special interest and impact on IO. The Navy has two

key organizations, the Fleet Information Warfare Center (FIWC) at Little Creek, Virginia, and the Naval Information Warfare Agency (NIWA) at Fort Meade, Maryland, dedicated to its efforts to develop IO. While the Marine Corps does not have a specific IO doctrine or organization, it sees IO as larger than merely another weapon or tool to be used when appropriate, as something that makes the entire range of Marine Corps capabilities and operations more efficient and effective. Finally, the Air Force has perhaps the most visionary approach to IO, with several doctrinal publications that explicitly focus on the information realm as an arena for combat and as an operational environment in which operations needed to be coordinated with and integrated into those in the air and outer space. It, too, has made organizational changes, and was the first service to dedicate an organization to the effort, recasting the existing USAF Electronic Warfare Center into the Air Force Information Warfare Center (AFIWC) in 1993.[36] None of these approaches are "right" or "wrong," but they do reflect the perspectives of warfare and warfighting held by their originating services. While some will see narrow parochialisms at work here, it would be more optimistic to think that from these differing perspectives will come a more robust, richer and more comprehensive concept for IW and IO than we have at present.[37]

In a simpler time, "joint" would have meant the four services acting in unison, but that is insufficient for effective IO. Not only are there a range of non-service DoD organizations that are critical to the military's ability to wage IW, using the previously-cited definition of IO means that virtually the entire apparatus of the federal government is involved in some way with the national security exercise of information power. While perhaps only a handful of federal organizations would be involved with CNA, others would be involved with CNE, and virtually every one with CND, because in the information age every organization is increasingly dependent on its electronic and computerized information networks for its efficient functioning. One of the most critical, if little-noticed, segments of PDD 63 was the tasking of each federal department or agency's chief information officer (CIO) with the responsibility for information assurance within that organization. This ties into another of PDD 63's critical actions, the assignment of specific segments of the government to work with their private sector counterparts (Department of Energy with the electric industry, for example) in developing the strategic partnership called for in the document. The latest National Security Strategy (December 2000) contains repeated references to the critical importance of safeguarding national infrastructures from intrusion or attack, whether that attack comes from the physical world or via CNA.

While some feel that the US military's interest in IW and IO is a reflection of a peculiar American affinity for technology and the degree in which information technology is embedded within our systems and structures, the growing interest of the rest of the world indicates that IW/IO is not solely an American issue. While this is neither the time nor place to make a detailed exploration of non-US perspectives on IW/IO, a few examples are in order. The British military has been pressing ahead both operationally and educationally, as have most of our other English-speaking allies, and their interest has included the pressing need to provide CND to counter the threat of CNA against vulnerable infrastructures.[38] Several other governments, including that of Norway, have undertaken specific PCCIP-type studies of their own national infrastructures because of the growing awareness that national security, including economic health and prosperity, depends on the smooth and confident functioning of these computer networks. The Swedish National Defense College (Forsvarshogskolan) has integrated IO into the core of its curricula, and the other Scandinavian countries are following suit. The Russian and Chinese perspectives have already been cited, albeit too briefly, and the views of one senior Indian national security strategist are enlightening. Major General Yashwant Deva recently wrote that the "metaterritorial" nature of IW was blurring the boundary between peace and war, and he argued that India's national security strategy must have an information strategy component to be effective.[39] These are perceptive insights from a country possessing the world largest "Silicon Valley" and one which is a global leader in information technology. Finally, the rapidly increasing use of cyberspace and computer networks for political objectives by nongovernmental organizations, whether they be humanitarian groups such as the Red Cross, political and environmental activists such as Greenpeace, or revolutionary groups such as the Tamil Eelam (Sri Lanka), Zapatistas (Mexico), or Hezbollah (Middle East), poses an interesting problem for governments and supra-national organizations that are uncomfortable working outside of the traditional and terrestrial boundaries of national security. In cyberspace all actors look somewhat alike, and as some recent incidents such as the Solar Sunrise case have illustrated, it can be very difficult to determine if the intruder is a lone individual or the agent of a State acting for State-sponsored purposes.

Concluding Thoughts

Those old enough to remember sayings and slang from the war in Southeast Asia may recall one that went "When you're up to your backside in alligators, it's kind of hard to remember that your initial mission was to drain the swamp."

Right now, in the field of information warfare, we are hip-deep in the swamp of unresolved issues, and there are a number of alligators circling. At the outset of this discussion we faced the Clausewitzian paradigm of warfare, which was based in part on the concept that wars are waged by "warriors" in service of identifiable States. In a postulated paradigm of war by keystroke, are those that operate from the keyboards to be considered "warriors?" We have seen examples in which young hackers, skilled at moving from database to database via cyberspace, never physically leaving their keyboards, have been inducted into the armed forces of their home countries.[40] Could this be used to provide a cadre of super-skilled operators who now have the technology of States at their fingertips, instead of what they can afford from Radio Shack? One thinks of the case of the Dutch hackers who vainly offered their services to Saddam Hussein during the Persian Gulf War. Could such individuals, if acting in the interests and behalf of a State, be considered cybermercenaries?[41] Equally plausible is the potential for them to act on behalf, not of a recognized State, but of some other interest group, whether it have political, religious, or even simply monetary motivations.

Our existing paradigm for war requires kinetic actions, destroying things, or crossing physical boundaries with physical objects such as airplanes or tanks. What are the political and legal regimes for actions that do not cross the physical limits of territorial sovereignty or cause kinetic destruction, but still have serious impact on the national security of the "attacked" State? Where are the lines of sovereignty in cyberspace, and how does the State respond to the provocations and intrusions of what may be a shadowy and virtual opponent? More and more of the key infrastructures that support civil society also support, in a strategic sense, the military power and capability of the State. Electric grids, oil and gas pipelines, transportation networks, and telecommunications are just some of those dual-use infrastructures and architectures that support both civil society and military strength. Those kinds of assets have been attacked and destroyed in wartime before, and they will be again, but what is the impact if the means of negation comes across the Internet in the forms of bits and bytes? Just as troubling is the question of who can and should defend those infrastructures? National armed forces protect them against attack by "traditional" military means, but does this mission extend into cyberspace? In the United States the answer from PDD 63 seems to be that this is a shared public sector-private sector responsibility that will require the coordination and cooperation of those communities to solve the problem of infrastructure vulnerability, but this may not necessarily be the answer in other countries that have different political-economic systems and traditions. These are just a sample of the questions and issues to be discussed and analyzed in the pages of this volume.

For more than a century and a half, from the era of Napoleon and Clausewitz, to that of strategic bombing and national liberation organizations, western political society has had a paradigm of warfare that has focused on the means employed: force and violence, employed to defeat or destroy the enemy's powers of physical resistance. Information "in war" is a continuation of this paradigm, and thus—as important as those capabilities are for the capability to employ traditional military force—is incomplete because of the new capabilities for influence, power, and the imposition of will offered by the new information technologies. Information warfare and information operations do not replace the older forms, but they do augment, modify, and change those forms. The difference between the terms is important, even vital, and we dare not ignore it, lest an adversary who lacks our bureaucratic and intellectual shackles and does not "understand our rules" use our very dependence on computer networks to administer a nasty strategic defeat via the very same environment and metanetwork we are so confidently constructing.

Notes

* The views expressed in this paper are those of the author and do not reflect the official policy or position of the National Defense University, the Department of Defense, or the United States Government

1. I am indebted to Lieutenant General Mike Hayden, Director of the National Security Agency—the DIRNSA—for this very descriptive phrase.

2. This author first met Dr. Rona and heard his concepts during a presentation on June 13, 1994, at the Information Resources Management College, National Defense University, in Washington DC. He defined IW as "*the sequence of actions undertaken by all sides in a conflict to destroy, degrade, and exploit the information systems of their adversaries. Conversely, information warfare also comprises all the actions aimed at protecting information systems against hostile attempts at destruction, degradation and exploitation. Information warfare actions take place in all phases of conflict evolution: peace, crisis, escalation, war, de-escalation and post conflict periods.*" Dr. Rona, a gentle man and brilliant analyst, unfortunately passed away in December 1997. For an example of his work, see Weapon Systems and Information War, a study prepared for Boeing in 1976.

3. This author vividly remembers the initial classroom meeting of the School of Information Warfare & Strategy's first group of students in August 1994, during which the sixteen students reacted with dismay to the plethora of official and unofficial definitions of information warfare. Some argue that any attempt to formally define IW is premature and counterproductive; others argue that some degree of consensus is essential, emphasizing that unless the different organizations that are involved in the issue have some common language and currency, any attempt to develop and execute plans and operations that not only span the entire government, but also involve the private sector and international community as well, are doomed to frustration and failure. While this author agrees that trying to put a "stone tablet on the wall" degree of finality on the terminology of IW is futile because the discipline is still evolving, some kind of terminological commonality is vital, even if it only provides a common target that all parties agree is "wrong."

4. While the Directive itself is classified Secret, this definition is unclassified.

5. One of the reasons for the creation of the term IO is the visceral dislike and mistrust of the word "war" by many of the agencies and people who are beginning to find that the information age envelops their activities and mission. Thus the creation of a term—IO—that points at the larger arena in which information activities are conducted, but does not tie those operations so visibly to the military and warfare.

6. See Chairman of the Joint Chiefs of Staff, Joint Publication 3-13, Joint Doctrine for Information Operations (1998), for these and other related definitions.

7. *See* Field Manual 100-6, Information Operations, (US Army Training and Doctrine Command, or TRADOC) (Aug. 1996); *see also* Air Force Doctrine Document 1, Air Force Basic Doctrine, (USAF Doctrine Center) at 31–32 (Sept. 1997); the Air Force's IO doctrine manual, AFDD 2-5, Information Operations (Oct. 1998).

8. *See* the author's Defining Information Power, Strategic Forum #115, Institute of National Strategic Studies, National Defense University, 1997, www.ndu.edu.

9. *See* National Security Decision Directive (NSDD) 130, US International Information Policy (March 6, 1984). The concept described above is based on NSDD 130, but paraphrases it and expands on some of its key components.

10. DANIEL R. HEADRICK, THE INVISIBLE WEAPON: TELECOMMUNICATIONS AND INTERNATIONAL POLITICS, 1851–1945, at 140–141 (1991). For Radio Free Europe's role, see Kevin J. McNamara, *Reaching Captive Minds with Radio*, ORBIS, Winter 1992, at 23–40; Walter Laqueur, *Save Public Diplomacy*, FOREIGN AFFAIRS, Sept.–Oct. 1994, at 24. For Russian views, see Tim Thomas, *Dialectical Versus Empirical Thinking: Ten Key Elements of the Russian Understanding of IO*, JOURNAL OF SLAVIC MILITARY AFFAIRS, March 1998 at 40–62.

11. While it is impossible to say when the term "cyberspace" was first used, several authors stand out as being among the leaders. William Gibson's classic work of science fiction, *Neuromancer* (1984), first raised the concept of humans seamlessly operating within a cybernetic, virtual-reality environment, while Nicholas Negroponte's book *Being Digital* (1995) is an exploration of the impact of cyberspace on our daily lives. The term itself has only recently come into widespread use. A search of several automated databases, for example, covering the years 1986–89 and 1986–91 contained only 17 "hits" on the term!

12. Of course, outer space can be measured in a scientific sense, but not in terms which are useful in a lay sense.

13. The question of where the borders of cyberspace lay is an intriguing one. Michael Benedikt has written perceptively on it in his book *Cyberspace: First Steps* (1991), while the late Anne Wells Branscomb in a recent monograph, Cybercommunities and Cybercommerce: Can We Learn to Cope? (Harvard University, Program on Information Resources Policy), suggested that the borders of cyberspace are discernible at the interconnection points between segments of the Internet, with network managers and systems administrators acting as the border guards, in a sense.

14. This construct omits communication methods such as signal flags, smoke signals, drums, or even heliograph because they did not require manipulation of the electronic environment.

15. THOMAS KUHN, THE STRUCTURE OF SCIENTIFIC REVOLUTIONS (1970).

16. This warning system used Air Force Space Command's space-based platforms to note Iraqi Scud missile launches; US Space Command to assess the indications; and Patriot missile systems operated by US Central and European Commands to engage the Scuds. This system thus crossed several physical boundaries (outer space, several oceans, the atmosphere, and cyberspace), national boundaries (the United States, Israel, and Saudi Arabia, at a minimum), and organizational boundaries (one service major command and at least three joint Unified Commands), all at the speed of light. This example illustrates a few of the capabilities, opportunities, and difficulties of warfare in the information age.

17. JV2010 is available electronically at www.dtic.mil/jv2010/.

18. This runs into the strawman view that since only a small minority of the world's population currently has immediate access to the Internet it is unimportant. One counter to this is that in 1776 only a certain segment of the American population supported the American Revolution, or could even read the Declaration of Independence, yet who would argue that document's political significance?

19. CJCSI 6510.1, Defensive Information Warfare Implementation (May 31, 1996).

20. Richard S. Berardino, SCADA and Related Systems: Critical and Vulnerable Elements of Domestic Components of National and Economic Security, unpublished research paper on file with author at National Defense University.

21. See the *Washington Post*, Feb. 24, 1996, at 4, for a detailed analysis of the accident.

22. For the PCCIP, see the Commission's report, Critical Foundations: Protecting America's Infrastructures, which at the time of this writing is electronically available via the website of the Commission's follow-on organization, the Critical Infrastructure Assurance Office, or CIAO, www.ciao.gov. The concept of "infrastructural warfare" has even generated an electronic journal, *The Journal of Infrastructural Warfare*, www.iwar.org.

23. *See also* Office of the General Counsel, Department of Defense, An Assessment of International Legal Issues in Information Operations (Nov. 1999). The paper is appended to this volume as the Appendix.

24. Two recent and very good examples of this are DOROTHY DENNING, INFORMATION WARFARE AND SECURITY (1998) and EDWARD WALTZ, INFORMATION WARFARE: PRINCIPLES AND OPERATIONS (1998).

25. *See* Lisa Hoffman, *US Opened Cyber-War During Kosovo Fight*, WASHINGTON TIMES, Oct. 24, 1999; Frederick H. Levien, *Kosovo: an IW Report Card*, JOURNAL OF ELECTRONIC DEFENSE (Sept. 1999), www.jedonline.com.

26. A lengthy and growing bibliography exists on the subject of infrastructure vulnerability. A recent contribution from the Center for Strategic and International Security (CSIS) is CYBERCRIME ... CYBERTERRORISM ... CYBERWARFARE ... AVERTING AN ELECTRONIC WATERLOO (1999); a growing number of official studies and reports echo this theme, including several from the General Accounting Office, as well as congressional hearings. *See, e.g.*, Security in Cyberspace: Hearings Before the Permanent Subcommittee on Investigations of the Committee on Governmental Affairs, US Senate, 104th Congress, May 22–July 16, 1996.

27. See CARL VON CLAUSEWITZ, ON WAR, Bk. 1, Ch. 1, for his complete analysis of these relationships.

28. See JAY LUVAAS, THE MILITARY LEGACY OF THE CIVIL WAR: THE EUROPEAN INHERITANCE (University of Kansas Press, 1988; originally University of Chicago Press, 1959) for the best discussion of how the European powers essentially ignored the lessons of the war of 1861–1865.

29. Actually, "Rosie" only built Liberty ships, not U-boats; one of the signal failures of the Nazi regime was its reluctance to significantly tap into this source of labor, one that the democracies fully exploited.

30. For a good discussion of this, see ED MANN, THUNDER AND LIGHTNING: DESERT STORM AND THE AIRPOWER DEBATES (1995).

31. For a discussion of the Air Force's doctrinal distinction between "information warfare" and "information in warfare," see Air Force Doctrine Document (AFDD) 2-5, Information Operations (1998).

32. *See China's Military Plots 'Dirty War' Against the West*, LONDON SUNDAY TELEGRAPH, Oct. 17, 1999; *see also* the longer explanation in the Foreign Broadcast Information Service translation from HONG KONG TA KUNG PAO, Sept. 19, 1999.

33. See the JV2010 website, *supra* note 17.

34. *See* DOMINANT BATTLESPACE KNOWLEDGE (Stuart J. Johnson & Martin C. Libicki, eds., 1995); DAVID S. ALBERTS, JOHN J. GARSTKA, & FREDERICK P. STEIN, NETWORK CENTRIC WARFARE: DEVELOPING AND LEVERAGING INFORMATION SUPERIORITY (1999). Both are available electronically via the DODCCRP website at www.dodccrp.org. The latter book is an expansion of the concept first promulgated by Admiral Arthur K. Cebrowski in *Network Centric Warfare*, US NAVAL INSTITUTE PROCEEDINGS, (Jan. 1998), at 28–35, www.usni.org.

35. For a fuller discussion of this, see the compilation of RMA-related articles in the Summer 1998 issue of JOINT FORCE QUARTERLY, www.dtic.mil/doctrine.

36. *See* Field Manual 100-6, Information Operations (1996); Chief of Naval Operations Publication, Navy Information Warfare Strategic Plan (1998); Major General J.E. Rhodes, *A Concept for Information Operations*, MARINE CORPS GAZETTE (Aug. 1998); USAF Doctrine Documents (AFDD) 1 and 2-5 (1997 and 1998 respectively). The USAF renamed the AFIWC as the AF Information Operations Center (AFIOC) in 2001.

37. See the author's Joint Information Warfare: a Paradigm for Information-Age Jointness, Strategic Forum #105, Institute of National Strategic Studies, National Defense University, March 1997, www.ndu.edu.

38. *See, e.g.*, Adam Cobb, Thinking About the Unthinkable: Australian Vulnerabilities to High-Tech Risks, Research Paper #18, 1997–98, Department of the [Australian] Parliamentary Library, Canberra, Australia, June 29, 1998.

39. Yashwant Deva, *National Perspective on Information War*, JOURNAL OF THE UNITED SERVICE INSTITUTION OF INDIA, Jan.– March 1998.

40. It is interesting that young Ehud Tenenbaum, the "Analyzer" from 1998's well-known Solar Sunrise incident, was called up for military service in the Israeli Defense Forces shortly afterwards. What service he is performing for the IDF is not known.

41. Only relatively recently in history have mercenaries acquired the general approbation which they now enjoy. After all, the first great victory of the American Continental Army, the day after Christmas, 1776, was at the Battle of Trenton. Washington's opponent: the Hessians, hired by the British crown.