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

XVII

Meeting the Challenge of Cyberterrorism: Defining the Military Role in a Democracy

Charles J. Dunlap, Jr.*

Headline grabbing events like the denial of service attacks[1] on "dot com" companies[2] in early 2000 and the excitement over 1999's Y2K fears[3] have served to turn public and governmental attention to the vulnerability of computers in an increasingly network-dependent, information-oriented society. For their part, militaries—and especially the US armed forces—have for some time been grappling with the implications of the metamorphosis spawned by the enormous advances in computer technologies of the last twenty years. A general consensus exists that emerging digital capabilities are stimulating what is popularly known as a "Revolution in Military Affairs," or RMA.[4] There are many aspects to the RMA,[5] but few would dispute that one progeny is the rise of information operations (IO)[6] as a specific military discipline.

In fact, the threat of cyberattack as a form of IO is a major concern of the US armed forces. In its doctrine, the military gives the defense of information systems open and prominent attention.[7] In military circles, IO is viewed as an asymmetric strategy because it presents an opportunity for an adversary with a narrow capability to successfully strike a seemingly more powerful opponent like the United States. One commentator explains this phenomena as follows:

> No other country or group can approach the US conventional-weapon superiority. This is why many terrorists find information terrorism an attractive alternative to traditional forms of terrorism. Cyber-terrorism allows terrorists—both foreign and domestic—to inflict damage with no harm to themselves and little chance of being caught. It is a way for the "weak" to attack the "strong," particularly to disrupt a stronger force at a key time during an operation.[8]

The threat of cyberterrorism as a form of IO is especially troublesome to the US armed forces because it can strike at vital systems not under military control. The Department of Defense (DoD) has officially acknowledged that today it is "dependent upon non-DoD assets—the international and national infrastructures, [and] other facilities and services of the private sector,"[9] and these could be targets of cyberattacks. The Air Force admits that this "Achilles' heel of the United States can be the great equalizer for a militarily inferior adversary."[10]

Still, "cyberterrorism" as a term of art does not, per se, find a home in the Pentagon's lexicon.[11] "Terrorism," however, is explicitly defined. The DoD describes it as "the calculated use of unlawful violence or threat of unlawful violence to inculcate fear; intended to coerce or to intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological."[12] Cyberterrorism might therefore be understood as using digital technologies to achieve the aims of traditional terrorism.

The purpose of this essay is to briefly outline the military's response to the threat of cyberterrorism, and to examine some of the emerging policy issues attendant to that response. In addition, I will discuss a few issues associated with using the tools of the cyberterrorist *against* America's enemies, and the complications that doing so presents to democratic societies. In addressing both these perspectives, I will be more concerned with identifying areas for further study than with presenting refined solutions. Having said that, I will attempt to anchor the discussion wherever possible in the context of American democracy and how it should shape the role of the military in addressing the dangers of cyberterrorism.

The Military Response

For at least five years, uniformed leaders have publicly discussed the vulnerability to cyberattack on the digital networks upon which the military relies.[13] Yet according to policy in place since 1995, the responsibility for the security of critical non-DoD "information systems and computer-based systems and networks that can be distributive in nature" remains with civilian law enforcement

authorities.[14] Nevertheless, the DoD "must be prepared, in concert with the appropriate authorities and within defense priorities, to assist in their protection" if the attack on the systems "seriously degrades or threatens DoD operations."[15]

Presidential Decision Directive (PDD) 63, issued in May of 1998,[16] provides a conceptual basis to expand DoD's responsibility. In that document DoD was designated as the "lead agency" in the area of "national defense" with responsibility for "coordinating all of the activities of the United States Government in that area."[17] PDD 63, however, left the scope of "national defense" undefined. In addition, PDD 63 established the National Infrastructure Protection Center (NIPC), an organization physically located within the Federal Bureau of Investigation (FBI).[18] NIPC brings DoD together with "representatives from the FBI, other US government agencies, state and local governments, and the private sector."[19] NIPC also serves as the US Government's "focal point for threat assessment, warning, investigation, and response for threats or attacks against our critical infrastructures."[20]

Paralleling these developments, the individual military services have taken steps to enhance defenses against cyberattacks. In 1993 the Air Force established the Air Force Information Warfare Center with the explicit mission of protecting friendly command and control systems.[21] The other services have likewise planned to confront a cyberadversary.[22] Further, the National Security Agency (NSA), an element of the Department of Defense, is tasked with an "information assurance mission."[23] In executing that mission, NSA "conducts defensive information operations, to achieve information assurance for information infrastructures critical to US national security interests." [24]

In order to further coordinate the military response, Joint Task Force Computer Network Defense (JTF-CND) was formed in early 1999[25] with a charter to orchestrate the protection of all DoD computer systems.[26] In a move to bolster its effectiveness, JTF-CND was placed under the control of US Space Command (USSPACECOM) in October of 1999.[27] At the same time, the Joint Information Operations Center was placed under SPACECOM control.[28] In another effort to increase its resources against cyberattack, the Defense Computer Forensics Lab was established in September 1999.[29] It aims to facilitate, among other things, the tracing across the Internet of hackers who threaten DoD systems.[30]

Finally, Joint Task Force-Civil Support (JTF-CS), an organization assigned to US Joint Forces Command, was established not to defend DoD systems per se, but to assist civilian authorities in managing the *consequences* of any catastrophic act of terrorism, including cyberterrorism. In announcing the new task force,

DoD conceded that the benign title of "civil support" and the selection of a National Guardsman instead of a Regular officer as the commander were both intended to quell the concerns of civil libertarians who feared that the "DoD was out to take over and would trample people's civil liberties" with the new organization.[31]

Although the armed forces were quietly developing an *offensive* IO capability for some time, it has only recently been discussed openly. Offensive IO embodies activities such as "operations security, military deception, psychological operations, electronic warfare, physical destruction and special information operations, and could include computer network attack."[32] These types of operations present a plethora of complex legal issues, and practical problems as well. DoD has admitted to Congress that during Operation ALLIED FORCE in Kosovo "the conduct of integrated information operations was hampered by the lack of advance planning and necessary strategic guidance."[33] In order to better focus the offensive information operations effort, General Richard Meyers, the commander of USSPACECOM, announced in January 2000 that effective October 1, 2000 the command will "pick up the computer network attack mission."[34]

The Emerging Policy Issues

Clearly, the US military aims to protect itself against cyberterrorism, facilitate a broader defense of US interests against that threat, and employ cybertechnology as a means and method of warfare, albeit for a presumably more righteous purpose than the cyberterrorist. What kind of policy issues should we expect to see?

Background

Before considering the specific issues associated with the role of the military in defending against cyberattacks, it is important to understand that in the US there is a generally accepted division of labor on security issues. As a rule, civilian law enforcement agencies handle internal security, while the primary purpose of the military is, as the Supreme Court put it in *Toth v. Quarles*, "to fight or be ready to fight wars should the occasion arise"—ordinarily an *externally* focused endeavor.[35] The tradition of ordinarily excluding the military from performing policing duties is traceable to the Founding Father's deep-seated suspicion of professional militaries.[36] That suspicion resulted from their cognizance of the excesses of Cromwell's New Model Army in England, as well as their loathing of

British regulars used to suppress the colonists' growing protests against imperial rule. For these and other reasons, the scheme for national security found in the Constitution principally contemplates not the large standing forces we have today, but a rather small number of regulars augmented by huge state militias.[37] In short, in practical terms it is doubtful that the Founding Fathers ever envisioned a standing army large enough to function as any kind of police force on a regular basis.

While the US military has been used successfully from time to time to quell civil disorders that overwhelm civilian resources, the record of the relatively few times it has been used for an extended period for a law enforcement-type mission is less than sanguine. Indeed, it was the intemperate behavior of Federal occupation troops during the post-Civil War Reconstruction Era that led to the passage of the Posse Comitatus Act in 1878.[38] The Act—which criminalizes the use of the military to enforce the law absent specific authority—remains the principle limitation on the employment of the armed forces for internal security purposes.

Of course, the Posse Comitatus Act is not intended to frustrate the military's ability to engage in bona fide national security-related activities. Exactly what constitutes a national security activity appropriate for military attention, however, became blurred during the Cold War, and especially during the domestic unrest of the Vietnam era. The result was an unwholesome involvement of the military establishment in the personal affairs of thousands of law-abiding US citizens. Professor Loch Johnson reports, for example, that "NSA computers were fed every single cable sent overseas by Americans from 1947 until 1975 [and] Army intelligence units conducted investigations against 100,000 Americans during the Vietnam War."[39]

The excesses of military and civilian intelligence agencies during this period led to Senate investigations in the 1970s (the Church Committee)[40] and substantial restrictions on the ability of military organizations to scrutinize US citizens.[41] Nevertheless, by the early 1980s the nation's drug crisis led Congress to enact a number of measures to involve the military in efforts to halt the tide of narcotics flowing into the country and to help stem the crime explosion catalyzed by illicit drugs.[42] While the armed forces are still generally prohibited from such activities as conducting searches and seizures and effecting arrests, the military counterdrug effort—especially in technical support and border surveillance activities—amounts to billions of dollars and involves thousands of uniformed personnel.

As a result of such initiatives, the traditional reluctance to employ the military in a domestic security role appears to be eroding. [43] Regrettably, however,

incidents occur that demonstrate that the skills of the soldier are not necessarily coterminous with those of the policeman. For example, the tragic 1997 shooting of a Texas high school sophomore by a Marine Corps border surveillance patrol may well illustrate that the orientation of the armed forces leads its members to deal with perceived threats differently than do law enforcement personnel.[44] This difference produces a very distinct approach to security problems.

As a general rule, soldiers move on threats by fire and maneuver with a view towards permanently eliminating them; police forces attach the presumption of innocence towards suspected lawbreakers and seek to resolve incidents peacefully with the ultimate disposition left to the courts. It should be no surprise, therefore—given the military's perspective—that a Pentagon-sponsored report argued that the Pentagon's "policy of prohibiting DoD from mounting a counter cyberattack if its computers are attacked puts the military at risk."[45] In responding to the report's proposal to allow the military to immediately launch a counterattack, John Pike of the Federation of American Scientists quipped, "Does this mean that the Pentagon will start frying the home PCs of American teen-age hackers?"

According to a 1999 Harris poll,[46] the armed forces enjoy a status as the most trusted institution in American society. In my opinion, few activities could jeopardize that trust more than an increased involvement in law enforcement and related activities that cause military personnel to intrude into the lives of everyday Americans. It would not seem to make sense, therefore, to involve military personnel in controversial proposals such as the Federal Intrusion Detection Network (FIDNET).[47] In an era when the US remains obliged by world events to maintain a still sizeable military establishment, and one that is now an all-volunteer professional force, the maintenance of harmonious civil-military relations ought to be a prime concern of democratic leaders. This is especially so given the troubling reports of a growing estrangement of the US armed forces from the nation it serves, notwithstanding the public's evident affection for those in uniform.[48]

Defending Against Cyberthreats

These lessons of the past are worth considering as we develop policies on the military's role in fighting cyberterrorism. Most experts agree that the nature of cyberterrorism is such that it is extremely difficult—at least initially and often later, if ever—to distinguish between the teenage hacker on a digital joy ride, the high-tech felon on a crime spree, the non-State cyberfanatics seeking to intimidate, and the nation-State waging information warfare. Moreover,

the clever cyberterrorist can often employ techniques that make it appear that innocent parties are the instigators of whatever chaos they manage to wreak. Thus, a military organization involved in investigating an attempted act of cyberterrorism could well find itself mistakenly probing innocent persons. Even when the guilty party is correctly identified, it may often be one more properly falling within the jurisdiction of a law enforcement agency, not a military force.

Consequently, the current policy that assumes—at the outset anyway—that an act of cyberterrorism is a criminal matter subject to law enforcement modalities as opposed to a hostile attack calling for a response by the armed forces seems appropriate. Moreover, military leaders—to include former Deputy Secretary of Defense John Hamre—have repeatedly emphasized that DoD is *not* seeking an active role in law enforcement in response to the terrorist threat.[49] Still, relative to the military, police resources are limited and diffused over thousands of jurisdictions. While this state of affairs may be satisfactory in the context of ordinary crime fighting requirements, it may be unacceptable if cyberterrorism presents a threat of truly catastrophic dimensions as some have claimed.

The magnitude of the cyberthreat has much to do with the appropriateness of a military response. A recent study[50] of the Posse Comitatus Act in relation to the protection of military and civil infrastructure against digital attack concluded that the military may conduct what might otherwise be considered prohibited law enforcement activities under certain circumstances. Specifically, action against civilians consistent with the act can occur when, *inter alia*, an "emergency" exists or when the activity is primarily in pursuit of a "military purpose."[51] Accordingly, "if the primary purpose of an action is to resolve or avert a problem with a strong tie to national security, the military purpose exception [to the Posse Comitatus Act] may be invoked."[52]

This brings us almost full circle to the central issue: when does cyberterrorism rise to the level of a true national security threat? We seem to accept almost without question the assertion that the US is "extraordinarily vulnerable" and that "an enemy could systematically disrupt banking, transportation, utilities, finance, government functions and defense."[53] To listen to many pundits, the US is virtually at the mercy of any teenager with a Radio Shack computer. The reality, I contend, is much different. Specifically, I believe that cyberterrorism—particularly when conceived exclusively in terms of computer network attack intended to cripple the nation's economy or military forces—is much more difficult to accomplish.

To put it bluntly, if cyberterrorism were so easy and cheap to do, why have we not seen a *catastrophic* event? If not in the US, anywhere? This is much the

same point that Rand analyst and cyberwar expert Martin Libicki wrote about in *Foreign Policy*.[54] In this regard, I think it would be a mistake to make too much of the past denial-of-service attacks on commercial sites. In the first place, most sites were impeded for only a short time, leading many experts to characterize the incidents as "little more than criminal mischief."[55] Ironically, the attacks may have caused little revenue loss. *Newsweek* wryly noted that since "dot-coms typically lose money on every sale they make, they might come out ahead" as a result of the attacks.[56]

As Libicki observes, there is a great difference between public commercial websites, and the sensitive military and civilian infrastructure operating systems whose incapacitation on a grand scale might stagger even a country like the United States. However vulnerable the former, the latter are much more secure and, in any event, often operate in a closed loop, independent mode requiring unique expertise even if access is somehow achieved. This is a key reason why, for example, Bruce F. Wollenberg, a professor of electrical engineering at the University of Minnesota, insists that the US power grid "isn't hacker friendly."[57]

Dan Kuehl, a respected professor at the National Defense University, argues that the reason a full-fledged cyberattack has not been launched is "solely because no state or non-nation state actor has yet seen sufficient strategic advantage to be gained by doing so—and this condition will not last indefinitely."[58] I disagree because I believe the requisite expertise is much rarer than many assume, and much of that expertise is on the side of the good guys. We live in a world of Saddam Husseins, Slobodan Milosevics, and Osama bin Ladens, who are hell-bent to inflict harm upon us in any way they can. These are people to whom the logic of "strategic advantage" is expressed in the most savage acts of terror they can manage to accomplish. They are smart, ruthless, moneyed, and motivated, yet have not achieved a crushing cyberassault.

We tend to discount too readily our own defensive capabilities. Recall that much was made of the supposed "hacker" capabilities of the allegedly computer-literate Serbs and others during the Kosovo campaign. Evidently, they tried hard. According to Lieutenant General William J. Donahue, "hackers came at us daily, hell-bent on taking down NATO networks."[59] Yet, the end result was failure: no NATO combat deaths, and a near-zero effect on the ultimate military outcome. Similarly, despite all the allegations of rampant, damaging attacks in the private sector, the reality is that the US economy continues to roar. Are we to believe that there are thousands of malicious people with diverse agendas at scores of locations around the globe fully capable of devastating us with keystrokes who are collectively refraining from doing so because of some serendipitously uniform appraisal of "strategic advantage"? My assessment of

human nature leads me to conclude otherwise. In short, they "would if they could—but they *can't.*"

Let me emphasize that I certainly do not counsel indifference; I recognize that cyberattacks will succeed occasionally. Collectively, they are costly—$7.6 billion in 1999 by one estimate.[60] Thus, I think the Clinton Administration's proposal to spend some $2 billion on various computer security programs is a prudent and affordable insurance policy for the nation.[61] I merely point out that as sizeable as the estimated cyber losses are, they must be understood in the context of a country that each year suffers more than $150 billion in costs from motor vehicle crashes alone[62]—not to mention over 40,000 deaths, and in excess of 6 million injured.[63] I simply caution that we should not unnecessarily divert resources from other pressing needs based on what may be an mistaken analysis of the threat.

Moreover, in calculating the dimensions of our potential cyberterrorism problem we should not underestimate the power of our capitalistic free market system to find solutions. In a very real way, America's military prowess is largely the product of its economic success. Given that business to business online sales are expected to grow to $1.3 trillion by 2003,[64] there is a immense incentive for the commercial development of reliable computer security technology for online transactions.

I believe the tremendous market imperative for secure transactions—and the incentive it creates for effective computer security products[65]—will rapidly outstrip the resources of individuals or even governments to create methodologies capable of circumventing improved defensive measures. In discussing the long-term threat after the denial-of-service attacks in early 2000, one commentator maintained that "[w]ith money at stake, e-businesses will fix this glitch."[66] Overall, I find persuasive Libicki's view that our "enemies best time to conduct information warfare has clearly come and gone."[67] All of this is yet more evidence that it is unnecessary at the present time to involve the military in cyberdefense any more than it is presently tasked.

To me, the real danger is not so much that cyberterrorists will use the Web as a vehicle for destructive computer network attacks, but rather that they will employ it as a convenient source of information useful for a variety of nefarious purposes. For example, I am convinced that cyberterrorists could gather enough personal information from Web sources to intimidate and harass individuals or even groups of individuals in the military and elsewhere. This is one reason that the DoD has begun to limit the amount of information available on public sites.[68] At least in the near term, however, the damage has been done. There is sufficient information already on the Internet for those disposed for whatever purpose to engage in such crimes as identity theft.[69] In fact, I believe

this problem is getting so difficult to rectify that in the not too distant future, courts will be adjudicating "identity replacement" much as they now do in bankruptcy cases. Still, these cyberthreats are, in my view, properly within the responsibility—and growing capability—of law enforcement agencies to resolve.[70]

Avoiding the Cyberterrorist Label

As important as it is to defend against cyberattacks, it is equally important to ensure that our own security activities avoid accusations that we ourselves are engaging in cyberterrorism. In a very real sense, the flip side of cyberterrorism is the use of cybertechniques for *legitimate* offensive IO. From the military perspective, the means and methods of the cyberterrorist are not necessarily *malum in se*; rather, they must be tested against existing domestic and international law applicable *ante bello* as well as *in bello*. Along this line, in 1999 the Office of the DoD General Counsel issued its first unclassified assessment of the legal aspects of information operations.[71] In other words, to the military way of thinking, cyberterrorism is objectionable because of its purposes and the *manner* in which it is employed (e.g., against noncombatants and noncombatant objects), not, per se, because of the techniques themselves.

Still, there are many legal and policy questions yet to be resolved. For example, what constitutes, in the layman's vernacular, the proverbial "act of war"? That is, what measure of peacetime cybermanipulation is tolerable before it amounts to a "use of force" or "armed attack" that plunges a nation into conflict?[72] While the definitive answer yet eludes us, there is a growing consensus that once the cyberassault creates consequences indistinguishable from that of a traditional kinetic attack, the legal status of the cyberevent becomes likewise the same.[73] Conversely, it appears cyberevents that do not reach that threshold would not therefore constitute aggression within the meaning of the UN Charter (although they may be violative of other aspects of international or domestic law).[74]

Reference to the UN Charter raises the larger issue of the wisdom of various suggestions for an international agreement addressing cyberterrorism. Some of these, like the Stanford proposal,[75] explicitly exclude "activities undertaken by military forces of a State party, or State party activities during armed conflict."[76] Others, like the reported Russian proposal, contemplate banning certain information weapons altogether.[77] Many would agree that there is a need for greater international cooperation to confront the unique issues presented by cyberterrorism[78] and that cooperation may need to take the form of an international agreement. That said, we ought to be cautious about entering into legal regimes that may unnecessarily hamper what is, after all, an area where the US, as the

world's foremost digital power, may itself have an asymmetric advantage across the spectrum of conflict.

To the extent news reports are reliable, the Kosovo conflict raised a number of interesting issues about the use of cybertechniques during armed conflict. For example, early in the campaign it was reported that a civilian US hacker sent a denial-of-service e-mail "bomb" that flooded the Serb Government website with 500,000 e-mails, crashing the site.[79] Is this person an unlawful combatant under international law? Likely. A cyberterrorist? Perhaps.

Additionally, it was widely reported in the press that senior policymakers did not approve a planned cyberassault of Milosevic's personal bank accounts.[80] I do not know if such a plan ever existed, let alone the reasons it was not executed.[81] If it did exist, however, one can imagine that a key issue would be the propriety of striking the private property of a civilian,[82] notwithstanding his position as the head of State of a belligerent. Given the growing aversion in the international community to the use of destructive, kinetic weapons in war that may cause civilian deaths, it may be useful to re-examine the prohibition against targeting of civilian objects via cybertechniques if bloodshed can be avoided through this kind of coercion. John Markoff, writing in the *New York Times*, argues that "cyberwarfare raises a fundamental philosophical question . . . the biggest challenge that such warfare may pose for democratic societies is that it further blurs the distinction between military and nonmilitary targets."[83]

There are other complex issues occasioned by emerging cyber capabilities for the armed forces of a democracy. In the US military, IO embraces a wide range of technology-empowered activities. Psychological operations, for example, are important to the military commander imbued in the Clausewitzean tradition to believe that the ability of an adversary to wage war depends upon the support of the "remarkable trinity" of the people, the government, and the armed forces.[84] Disassembling the enemy's trinity, that is, undermining his *will* while preserving one's own, is an accepted military objective.[85]

Some emerging cybertechniques present exciting opportunities for the military professional to sap an enemy's resolve with relatively little violence.[86] As Hollywood has repeatedly demonstrated, the ability to use digital means to morph or otherwise create extremely convincing—but false—images is now widely available.[87] Considering such capabilities, Thomas Czerwinski, then a professor at the National Defense University, posed an interesting question: "What would happen if you took Saddam Hussein's image, altered it, and projected it back to Iraq showing him voicing doubts about his own Baath Party?"[88] Quite obviously, it could deceive a population about its leaders, as Professor Czerwinski indicates.

Few would call such efforts against a totalitarian or wholly depraved regime "cyberterrorism." A different issue arises, I believe, when the hostile government is a genuinely democratic one. Consider that if Internet-based voting—which the US military is experimenting with today[89]—becomes widespread, the potential exists to manipulate elections in enemy countries during armed conflict via cybersubversion of the voting process itself.

Would such an operation be appropriate in light of US national security policy that promotes democracy?[90] I do not think so, even though I am not an adherent to the democratic peace theory.[91] Based on my own experience in Somalia and elsewhere, I find Professor Samuel P. Huntington's "clash of civilizations" thesis far more convincing.[92] I accept that there are entire societies that hold values fundamentally different from our own—and they would freely vote to retain those values—even though the policies they produce may lead to conflict with the US or other Western nations.[93] Nevertheless, I also believe that democracy ought not to be asked to "pay for itself," so to speak, by necessarily producing peace.

Democracy as an expression of the principle of self-determination found in the UN Charter[94] and elsewhere has an intrinsic human value independent of any peace-generating quality. Accordingly, is it right to apply cybertechniques against an adversary's democratic *processes*, even in time of war? Certainly it is appropriate to act to control the hostile acts of any government, democratic or otherwise. It seems to me, however, that care must be taken to distinguish between the use of cyberweapons to address the *actions* of a democratic government, and employing them to undermine the democratic *processes* that produced it.

Michael Walzer, perhaps the premier ethicist on issues of war and peace, gives us another matter to consider. He points out that, excluding exceptional cases like Nazi Germany, war aims "don't legitimately reach to the transformation of the internal politics of the aggressor state or the replacement of its regime."[95] In other words, we must be very cautious in employing advanced digital methodologies that may destroy the confidence of people in democratic processes.

Consider also the other vital part of the Clausewitzean trinity: maintaining the will of the publics of *friendly* countries.[96] This is especially a concern for democratic countries, and it was raised during the Kosovo operation. You may recall that Serb radio and television stations were bombed in attacks highly criticized by Human Rights Watch[97] and others.[98] In my opinion, the attacks were warranted[99] since it appears that the facilities were used to whip up ethnic hatred for years.[100] As Air Commodore David Wilby, a NATO spokesman, explained on April 8, 1999, "Serb radio and TV is an instrument of propaganda and repression. . . . It is . . . a legitimate target in this campaign." [101] Since, *inter alia*,

incitement to genocide may itself be a war crime,[102] Wilby's assertions seem to have merit, assuming the other prerequisites of the law of armed conflict were met.

If cybertechniques can neutralize the facilities without the physical destruction conventional munitions cause, we should embrace netwar as a development that could reduce the misery of war. Suppose, however, that the enemy radio and television stations were transmitting not propaganda, per se, but accurate information about US operations that nevertheless was eroding support among our public or that of allied democracies?[103] For example, in a report on the attacks on Serb television stations, Patrick L. Sloyan observed that while bombing stopped the "diet of lies fed Serb viewers," it also served to "curb transmission to the West of those disturbing 'collateral damage' pictures that could erode public support for NATO's escalating strikes in the Balkans."[104] If addressing the latter concern were the *sole* aim—as opposed to, for example, the limited notion of preserving operational security in a particular circumstance—would the attacks be justified? Probably not.

Censorship and exclusion of the press from military operations has long been tolerated in liberal democracies during wartime.[105] Essentially, where there is a demonstration that the information would present a clear and present danger to national security, it could be suppressed.[106] That concept, however, would not seem to permit the suppression of news reports—via cyberassault or other means—simply because the information conveyed would tend to demoralize public opinion in our own country, or that of our allies. Democracy, I believe, has its price.

Concluding Observations

If this brief survey has succeeded, the reader will appreciate that the issues raised by cyberterrorism are many and complex. At the present time, law and policy carefully circumscribe the military's role, and to date DoD has been careful to stay within those limits.[107] There are, however, calls for expanded responsibility. Some suggest a relaxation of the policy that presumes at least initially that a cyberattack is a civilian law enforcement problem, not a national security issue.[108] Doing so, it is contended, would allow that application of the considerable resources of the military and intelligence communities that currently are barred from use in most domestic cases involving US persons.[109]

To this end, one innovative proposal calls for a policy that presumes the digital "intruder is *not* a US person," thus permitting "the full capabilities of the United States' investigative and intelligence assets" to be brought to bear.[110] However, this reversal of the present presumption would apply only to attacks

against specified systems that are deemed by statute to be critical to the nation's economic and national security interests.[111] Whether such an approach is politically feasible depends upon public perceptions. As already indicated, what role, if any, the military should play in defending against domestic cyberattacks is embedded in the larger issue regarding the extent to which Americans believe their way of life is put at risk by the potential of cyberterrorism.

In this regard, I would add one final note of caution. I have often heard a variety of senior Pentagon[112] and national security officials[113] insist that the US is susceptible to an "electronic Pearl Harbor." Conjuring up emotional images of the infamous sneak attack that pulled the US into World War II is certainly an effective way to hype the interest of persons both in and out of uniform towards greater vigilance and preparedness. The analogy is one plainly worth pondering, especially as our society becomes increasingly digitally dependent.

There is, however, a very dark side of the Pearl Harbor story that we should also keep in mind. As a result of the fears generated, the US military—acting in a domestic security role—rounded up thousands of loyal American citizens and placed them in detention camps, all in the name of responding to a threat to national security. We know today that the sacrifice of the rights of Japanese-Americans was wholly unnecessary. Although it may be fashionable these days to say that the roundups were simply racism run amok, those that have actually read *Korematsu v. United States*,[114] as well as Chief Justice Rehnquist's discussion in his recent book[115] may conclude otherwise. From those sources one can reasonably conclude that principled men struggling with a real fear of invasion by an enemy who had already demonstrated his treachery at Pearl Harbor made what they sincerely believed was a unavoidable decision—however wrongheaded it appears with the benefit of hindsight.

But, in a sense, the fact that *respectable* people were nevertheless responsible for the treatment of Japanese-Americans that we now find so objectionable should itself give us pause. As we consider the growing involvement of the military in countering cyberterrorism, we must never forget that the armed forces is the least democratic and most unapologetically authoritarian element of our society. I hasten to add that this does not presume anything sinister about those in uniform or those that advocate an enhanced role for the military in fighting cyberterrorism. I merely submit that in a democracy, and especially American democracy, the machinations of the truly evil are, somewhat paradoxically, frequently more readily corrected than are the misdirected efforts of well-intentioned, honorable citizens.

Pearl Harbor and the sacrifices that followed in its aftermath remain a lesson for us as we consider what role, if any, the military should play in countering

cyberterrorism. On a deeper level we must accept that perfect security is fundamentally at odds with democratic values. This applies as much to cyberterrorism as to any other threat against us. We must be prepared to take prudent risks in order to have a free society. The inescapable truth is that we must likewise acknowledge that from time to time our freedom will exact a harsh price from us and those we love.

Nevertheless, we must not allow the dread of digital terror to drive us to take counsel of our fears. As Martin Van Creveld and others have pointed out, terrorism has not succeeded in developed States because it is a characteristic of modernity to have a robust level of technological redundancy and political resiliency so as to make individual terrorist attacks relatively futile in terms of real effect on capability.[116] While cyberterrorists might be able to inflict costly losses periodically, they cannot physically imperil our continued existence as a free nation. Indeed, the *real* risk is upon those who challenge the forces of freedom. As Professor Victor Hanson explains in his book, *Soul of Battle,*[117] history shows that the forces of democracies *once aroused* are extraordinarily fearsome combatants who, notwithstanding the seeming empowering militarism of the opposing forces, tend to not merely defeat the armies of despots, but to pulverize them *and everything that supports them.* So profound is such defeat that the very societies that produced the forces of tyranny are left fundamentally changed and virtually unrecognizable to their former masters. The enemies of democracies ought to take note.

In summary, the true threat is not what damage cyberterrorists can inflict upon our digital systems, but what freedoms they can force us to forfeit. The *San Francisco Chronicle,* citing a report by the Commission on National Security/21st Century,[118] editorialized that "terrorist hackers" and other threats "will probably put pressure on the military to move into domestic law enforcement, blurring the line between domestic and foreign threats."[119] It soberly warned "it is better to live with danger than in the security of a police State."[120] Although we are certainly not yet living in the shadow of a police State, it is a timely reminder of what is really at stake.

Notes

* The views and opinions expressed in this chapter are those of the author alone and do not necessarily represent those of the US Government or any of its components.

1. *See, e.g.,* Brendan I. Koerner, *The Web's Bad Week,* U.S. NEWS & WORLD REPORT, February 21, 2000, at 19 ("The intruder used an elementary method know as a denial of service attack, which cripples a network by flooding it with too much information.").

2. "Dot com" is a generic name for companies whose business is integrated with the Internet.

3. "Y2K" is shorthand for "Year 2000" and refers to the anomaly in some software programs that causes dates after 1999 to be misread resulting in erroneous calculations. For information on the Department of Defense program to address Y2K, see www.defenselink.mil/issues/y2k.html.

4. For a discussion as to how the "Revolution in Military Affairs" (RMA) interplays with cyberwar, see Sydney J. Freedberg, *Future-Shock Troops*, NATIONAL JOURNAL, December 11, 1999, ebird.dtic.mil/Dec1999/s19991212future.htm.

5. For an overview of how the military intends to incorporate the RMA, see Chairman of the Joint Chiefs of Staff, Joint Vision 2010 (1996), www.dtic.mil/jv2010/jvpub.htm.

6. "Information operations" is defined as "actions taken to affect adversary information and information systems while defending one's own information and information systems." *See* Chairman of the Joint Chiefs of Staff, Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms (2001), www.dtic.mil/doctrine/jel/ref.htm, [hereinafter JP1-02]. "Information warfare" is "information operations conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries." *Id.*

7. *See, e.g.*, Chairman of the Joint Chiefs of Staff, Joint Publication 3-13, Joint Doctrine for Information Operations, ch. III (1998).

8. Tom Regan, *When Terrorist Turn to the Internet*, CHRISTIAN SCIENCE MONITOR, July 1, 1999, at 1.

9. US Department of Defense Directive, Critical Asset Assurance Program (CAAP) 5160.54, January 20, 1998, para. 4.2.

10. Department of the Air Force Doctrine Document 2-5, Information Operations, August 5, 1998, at 6.

11. Barry Colin, a senior research fellow at the Institute for Security and Intelligence, claims to have coined the term "cyberterrorism." *See* Pacific Air Force News, *Terror Can Be Just a Computer Away*, Release No. 98013, February 5, 1998, www2.hickam.af.mil/news/newsarchive/1998/98013.htm.

12. JP 1-02, *supra* note 6.

13. *See, e.g.*, General Ronald R. Fogleman, Information Operations: The Fifth Dimension of Warfare, DEFENSE ISSUES, April 25, 1995, defenselink.mil/speeches/1995/s19950425-fogleman.html.

14. *Id.* at para. 4.3.

15. *Id.*

16. The White House, White Paper, The Clinton's Administration Policy on Critical Infrastructure Protection: Presidential Decision Directive 63, May 22, 1998, [hereinafter PDD 63], press release summary available at www.pub.whitehouse.gov/uri-res/I2R?urn:pdi://oma.eop.gov.us/1998/5/26/1.text1.

17. *Id.* at 4 & 8.

18. *Id.* at 10.

19. Michael Vatis, Director of the National Infrastructure Protection Center, Message from Michael Vatis, www.fbi.gov/nipc/welcome.htm.

20. *Id.*

21. The AFIC home page is available at www.aia.af.mil/common/homepages/pa/bios/iwcfact.html.

22. The Navy has the Fleet Information Warfare Center website available at www.fiwc.navy.mil/html/home.html, and the Army has the Information Assurance Directorate website available at www.army.mil/disc4/isec/c2p/mission/mission.htm.

23. National Security Agency, Mission Statement, available at www.nsa.gov/about_nsa/mission.html.

24. *Id.*

25. Office of the Assistant Secretary of Defense (Public Affairs), Joint Task Force On Computer Network Defense Now Operational, December 30, 1998, (press release), www.defenselink.mil/news/Dec1998/b12301998_bt658-98.html.

26. *See* Frank Wolfe, Joint Task Force To Direct Pentagon's Cyber Defense, DEFENSE DAILY, January 26, 1999, at 1.

27. US Space Command, USSPACECOM Takes Charge of DoD Computer Network Defenses, Release No. 19-99, October 1, 1999 (press release), www.spacecom.af.mil/usspace/new19-99.htm.

28. US Space Command, Joint Information Operations Center Joins USSPACECOM, Release No. 20-99, October 1, 1999 (press release), www.spacecom.af.mil/usspace/new20-99.htm.

29. Douglas J. Gilbert, High-Tech Lab Ties Computers to Crimes, American Forces Press Service, November 1999, www.defenselink.mil/news/Nov1999/n11021999_9911023.html.

30. *Id.*

31. Linda D. Kozaryn, DoD Helps Hometown USA Confront Terrorism, American Forces Press Service, January 2000, www.defenselink.mil/news/Jan2000/n01132000_20001133.htm.

32. JP 1-02, *supra* note 6.

33. Department of Defense, Report to Congress: Kosovo/Operation Allied Force After-Action Report, January 31, 2000, at 99, www.defenselink.mil/pubs/kaar02072000.pdf.

34. General Richard Myers, Special Briefing re: Current Activities of U.S. Space Command, January 5, 2000 (DoD News Briefing), www.defenselink.mil/news/Jan2000/t01052000_t104myer.html.

35. *Toth v. Quarles*, 350 U.S. 11, 17 (1955).

36. For a discussion of the author's views of this issue, see generally Charles J. Dunlap, Jr., *Revolt of the Masses: Armed Civilians and the Insurrectionary Theory of the Second Amendment*, 62 TENNESSEE LAW REVIEW 643 (1995).

37. *Id.* at 648649.

38. Act of June 18, 1878, ch. 263, § 15, 20 Stat. 152 (current version at 18 US Code § 1385 (Supp. 1999)).

39. LOCH K. JOHNSON, A SEASON OF INQUIRY 223 (1985).

40. *See generally, id.*

41. *See, e.g.*, Foreign Intelligence Act of 1978, 50 U.S.C.A. §§ 1801-1811 (1991) and Exec. Order No. 12,333, 46 FEDERAL REGISTER 59,941 (1981) (limiting, *inter alia*, the use of intelligence agencies including those of the armed forces to collect information on persons within the US).

42. *See, e.g.*, Department of Defense Authorization Act, Pub. L. No. 97-86, § 905(a)(1), 95 Stat. 1099, 1115 (1981), amended by National Defense Authorization Act, Pub. L. No. 100-456, § 1104(a), 102 Stat. 1918, 2043 (1988); National Defense Authorization Act for Fiscal Year 1990 and 1991, Pub. L. No. 101-189, § 1216(a), Nov. 29, 1989, 103 Stat. 1352, 1569 (codified at 10 US Code § 371-380 (1988).

43. *See generally*, Charles J. Dunlap, Jr., *The Police-ization of the Military*, 27 JOURNAL OF POLITICAL AND MILITARY SOCIOLOGY 217 (1999).

44 *Id.*

45. *See* Bob Brewin, *Report: Allow Cyberwar Response*, FEDERAL COMPUTER WEEK, March 29, 1999 (citing a report by the National Resource Council), www.fcw.com/fcw/articles/1999/FCW_032999_255.asp.

46. *See* www.usarec.army.mil/hq/apa/slides/VIPRecruitingbrief/tsld006.htm. *See also* Robert Burns, *Poll: Americans Appreciate the Armed Forces*, PACIFIC STARS AND STRIPES, October 19, 1999, at 1.

47. FIDNET is designed to "protect vital systems in federal civilian agencies, and to ensure the rapid implementation of system 'patches' for known software defects." *See* White House, Office of the Press Secretary, Cyber Security Budget Initiatives, February 15, 2000, www.whitehouse. gov/WH/New/html/20000215_1.html. FIDNET is controversial becomes some believe it would be improperly monitoring citizens, a charge the government has denied. *See* Tim Weiner, *Author of Computer Surveillance Plan Tries to Ease Fears*, NEW YORK TIMES, August 16, 1999, ebird.dtic.mil/Aug1999/s19990817author.htm.

48. *See, e.g.*, Triangle Institute for Security Studies, Project on the Gap between Military and Civil Societies, Digest of Findings and Studies, October 1999, www.unc.edu/depts/tiss/CIVMIL.htm.

49. John J. Hamre, *U.S, Military Wants No Domestic Law Enforcement Role*, USA TODAY, October 5, 1999, at 16 (letter).

50. Gregory Grove, Center for International Security and Cooperation, Stanford University, The U.S. Military and Civil Infrastructure Protection: Restrictions and Discretion under the Posse Comitatus Act 23 (1999).

51. *Id.*

52. *Id.* at 25.

53. Bob Drogin, *In Theory, Reality, U.S. Open to Cyber-Attack*, LOS ANGELES TIMES, October 9, 1999, at 16, www.latimes.com/archives/, *quoting* Richard Clarke, National Coordinator for Security, Infrastructure Protection and Counterterrorism.

54. Martin Libicki, *Rethinking War: The Mouse's New Roar?*, FOREIGN POLICY, Winter 1999/2000, at 30 (abstract available at www.foreignpolicy.com/articles/winter1999-2000/Libicki.htm).

55. *See* Anne Plummer, *Pentagon Response To Commercial Denial-of-Service Attacks Limited*, DEFENSE INFORMATION AND ELECTRONICS REPORT, February 18, 2000, at 1.

56. Steven Levy & Brad Stone, *Hunting the Hackers*, NEWSWEEK, February 21, 2000, at 38, 44, newsweek.com/nw-srv/printed/us/st/a16375-2000feb13.htm.

57. Bruce F. Wollenberg, *The U.S. Power Grid Isn't Hacker-Friendly*, WASHINGTON TIMES, April 22, 1998, at 18 (letter).

58. Vernon Loeb, *Cyberwar's Economic Threat*, WASHINGTON POST, February 24, 2000, at 19, *quoting* Dan Kuehl.

59. Bob Brewin, *General: Cyberattacks against NATO traced to China*, FEDERAL COMPUTER WEEK, September 1, 1999, www.fcw.com/fcw/articles/1999/fcw_09011999_china.asp.

60. John J. Stanton, *Rules Of Cyberwar Baffle U.S. Government Agencies*, NATIONAL DEFENSE, February 2000, at 29, ebird.dtic.mil/Feb2000/s20000208rules.htm.

61. *See* White House, Cyber Security Budget Initiatives, *supra* note 47.

62. *See* National Highway Traffic Safety Administration, The Economic Cost of Motor Vehicle Crashes, 1994 (1995), www.nhtsa.dot.gov/people/economic/ecomvc1994.html.

63. Per e-mail with Michael Baxter, Insurance Institute of Indiana, March 15, 2000 (on file with author).

64. Deborah Shapley, *Dr. E-Mail Will See You Now*, TECHNOLOGY REVIEW, January/February 2000, at 42, 44 (*citing* Forrester Research), www.techreview.com/articles/jan00/shapley.htm.

65. In the aftermath of the denial-of-service attacks, Philip H. Karns, an engineer at Qualcom Corp., reports that the "Internet industry experts are rushing the development of software that will locate, trace, and block future denial-of-service attack. . . ." David E. Rovella, *Preparing for a New Cyberwar*, NATIONAL LAW JOURNAL, March 13, 2000, www.lawnewsnetwork.com/stories/A18373-2000Mar10.html.

66. Allan Sloan, *Why the Market Will Rule*, NEWSWEEK, February 21, 2000, at 49, newsweek.com/nw-srv/printed/us/st/a16331-2000feb13.htm (visited March 15, 2000).

67. *See* Libicki, *supra* note 54.

68. *See* John Diamond, *Pentagon Reconsidering What To Make Available on Web*, PACIFIC STARS AND STRIPES, February 18, 1999, at 1.

69. *See, e.g.*, Thomas Ricks, *The Pentagon Says Web Site Made Credit-Card Scam Easier*, WALL STREET JOURNAL, December 8, 1999, at 1.

70. *See, e.g.*, Eric Yoder, *The CyberForce*, GOVERNMENT EXECUTIVE, February 2000, at 45 (describing the growing number of specially trained federal employees involved in Internet law enforcement), www.govexec.com/features/0200/0200s5.htm.

71. *See* Office of General Counsel, Department of Defense, An Assessment of International Legal Issues in Information Operations (Nov. 1999) [hereinafter DoD/GC Paper]. The paper is appended to this volume as the Appendix.

72. The UN Charter requires members to "refrain from the use of force threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations." UN CHARTER art. 2, para. 4. In addition, members are authorized to use force in self-defense if they are the victims of an armed attack. *Id.*, art. 51.

73. *See, e.g.*, WALTER GARY SHARP, SR., CYBERSPACE AND THE USE OF FORCE (1999) and Michael N. Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 COLUMBIA JOURNAL OF TRANSNATIONAL LAW 885 (1999).

74. *See generally*, James N. Bond, *Peacetime Data Manipulation as One Aspect of Offensive Information Warfare: Questions of Legality under the United Nations Charter Article 2 (4)* (1996) (unpublished paper, Naval War College) (on file with author).

75. Center for International Security and Cooperation, Stanford University, Draft International Convention to Combat Cyber Crime and Cyber Terrorism (1999), www.stanford.edu/group/ CISAC/test/research/Draft.html.

76. *Id.*, art. 20.

77. *See* Bradley Graham, *Military Grappling With Rules for Cyber Warfare*, WASHINGTON POST, November 8, 1999, at 1 (discussing Russian efforts to "gather support for a United Nations resolution calling for new international guidelines and the banning of particularly dangerous information weapons").

78. *See, e.g.*, Richard Hill, *Legal Obstacles Compound Pentagon's Cyberwar Challenges*, DEFENSE INFORMATION AND ELECTRONICS REPORT, March 12, 1999, at 1, ebird.dtic.mil/Mar1999/ s1999/s19990315legal.htm.

79. Patrick Riley, E-Strikes and Cyber-Sabotage: Civilian Hackers Go Online to Fight, April 15, 1999, Foxnews Online, available at www.foxnews.com/world/041599/ Kosovoside_hackers.sml.

80. *See, e.g.*, Gregory L. Vistica, *Cyberwar and Sabotage*, NEWSWEEK, May 31, 1999, at 38.

81. *See* William Arkin, *Cyber Bomb in Yugoslavia*, WASHINGTON POST (Electronic Edition), Oct. 25, 1999, and Bradley Graham, *Military Grappling With Rules For Cyber Warfare*, WASHINGTON POST, Nov. 8, 1999, at 1.

82. *See* Protocol Additional I to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts, art. 51, 1125 U.N.T.S. 3, 16 INTERNATIONAL LEGAL MATERIALS 1391, 1413 (forbidding attacks on civilian objects). While the US has not ratified Protocol I, the US recognizes many of its provisions as customary international law or accepted practice. This acceptance includes the provisions of Article 51 with the exception of paragraph 6 regarding reprisals. International and Operational Law Department, The Judge Advocate General's School, United States Army, OPERATIONAL LAW HANDBOOK, 5-2 (2000).

83. John Markoff, *Cyberwarfare Breaks the Rules of Military Engagement*, NEW YORK TIMES, October 17, 1999, at 23.

84. CARL VON CLAUSEWITZ, ON WAR 89 (Michael Howard and Peter Paret eds. and trans., 1976) (1832).

85. Clausewitz observed that war is an act intended "to compel our enemy to do our will." *Id.* at 75.

86. The author has previously discussed this theme. *See* Charles J. Dunlap, Jr., *Technology: Recomplicating Moral Life for the Nation's Defenders*, PARAMETERS, Autumn 1999, at 24, 37–38.

87. *See generally*, William M. Arkin, *When Seeing and Hearing Isn't Believing*, WASHINGTON POST (online edition) February 1, 1999, www.washingtonpost.com/ wp-srv/ national/dotmil/ arkin020199.htm.

88. *As quoted by* Peter Grier, *Information Warfare*, AIR FORCE MAGAZINE, March 1995, at 35.

89. *See, e.g.*, Lisa Hoffman, *U.S. Troops Serving Abroad To Try Out Cyber-Voting Option*, WASHINGTON TIMES, Nov. 28, 1999, at C4, ebird.dtic.mil/Feb1999/e19990217web.htm.

90. The White House, A National Security Strategy for a New Century 19 (May 1997).

91. *See, e.g.*, R.J. RUMMEL, POWER KILLS: DEMOCRACY AS A METHOD OF NONVIOLENCE (1997).

92. Huntington's original thesis (first published in 1993), together with thoughtful critiques have been published. *See* COUNCIL ON FOREIGN RELATIONS, THE CLASH OF CIVILIZATIONS? THE DEBATE (1996). His book-length treatment is entitled THE CLASH OF CIVILIZATIONS AND THE REMAKING OF WORLD ORDER (1995).

93. The author has discussed this theme on several occasions including: Charles J. Dunlap, Jr. *Preliminary Observations: Asymmetrical Warfare and the Western Mindset*, in CHALLENGING THE UNITED STATES SYMMETRICALLY AND ASYMMETRICALLY: CAN AMERICA BE DEFEATED? (Lloyd J. Matthews, ed., 1998), carlisle-www.army.mil/usassi/ssipubs/pubs98/ chalngng/chalngng.htm.

94. *See* UN CHARTER art. 1, para 2. *See supra* note 72.

95. MICHAEL WALZER, JUST AND UNJUST WARS XVII (2d ed. 1992).

96. *See supra* notes 84 and 85, and accompanying text.

97. Human Rights Watch (HRW), Civilian Deaths in the NATO Air Campaign, HRW Report, February 7, 2000, at 22-23, xmail.hrw.org/nato/Matbm200-01.htm.

98. *See, e.g.*, Walter J. Rockler, *War Crimes Law Applies to the U.S. Too*, CHICAGO TRIBUNE, May 23, 1999, ebird.dtic.mil/May1999/e19990525warcrimes.htm.

99. According to the DoD General Counsel, "[w]hen it is determined that civilian media broadcasts are directly interfering with the accomplishment of the military force's mission, there is no law of war objection to using minimum force to shut it down." *See* DoD/GC Paper, *supra* note 71.

100. *See, e.g.*, Jamie F. Metzl, *Information Intervention*, FOREIGN AFFAIRS, November/ December 1997, at 15.

101. *See* William M. Arkin, *Changing the Channel in Belgrade*, WASHINGTON POST (online edition), May 25, 1990, *quoting* Air Commodore David Wilby, www.washingtonpost.com/ wp-srv/national/dotmil/arkin052499.htm.

102. *See generally*, LAWRENCE T. GREENBERG, SEYMOUR E. GOODMAN, & KEVIN J. SOO HOO, INFORMATION WARFARE AND INTERNATIONAL LAW 36 (1998).

103. With respect to *adversary* news outlets, the DoD General Counsel states that the "extent to which force can be used for purely psychological operations purposes, such as shutting down a civilian radio station for the sole purpose of undermining the morale of the civilian population, is an issue that has yet to be addressed authoritatively by the international community." *See* DoD/GC Paper, *supra* note 71.

104. Patrick L. Sloyan, *The Fog of War*, AMERICAN JOURNALISM REVIEW, June 1999, ebird.dtic.mil/Jun1999/s19990608fog.htm.

105. *See generally*, John Calvin Jeffries, Jr. *Excluding the Press from Military Operations, in* NATIONAL SECURITY LAW 993 (John Norton Moore, Frederick S. Tipson, & Robert F. Turner eds., 1990).

106. *See generally*, Donald L. Robinson, *National Security*, *n* THE OXFORD COMPANION TO THE SUPREME COURT 574 (1992).

107. *Cf.* Robert L. Deitz, *NSA Obeying the Law*, WASHINGTON POST, Dec. 7, 1999, at 30, ebird.dtic.mil/Dec1999/s19991207nsa.htm.

108. *See, e.g.*, Catherine MacRae, *Cybercrime Vs Cyber Terrorism, DoD Official Says U.S. Has Been Victim Of Cyber Crimes, Not Terrorism*, DEFENSE INFORMATION AND ELECTRONICS REPORT, Oct. 1, 1999 (*citing* James Christy, law enforcement and counterintelligence coordinator for the DoD Information Assurance Program), www.infowar.com/ mil_c4i/99/ mil_c4I_j.shtml.

109. *See supra* note 41, and accompanying text.

110. Walter Gary Sharp, Sr., *Balancing Our Civil Liberties with Our National Security Interests in Cyberspace*, 4 TEXAS REVIEW OF LAW & POLITICS 69, 72–73 (1999) (emphasis in the original).

111. *Id.*

112. *See* Jim Garamone, Hamre "Cuts" Op Center Ribbon, Thanks Cyberwarriors, American Forces Information Services, Aug. 1999, www.defenselink.mil/news/Aug.1999/ n08241999_9908241.html, quoting former Deputy Defense Secretary Hamre ("Several times I've testified and talked about the future electronic Pearl Harbor to the United States.")

113. Tim Weiner, *Author of Computer Surveillance Plan Tries to Ease Fears*, NEW YORK TIMES, August 16, 1999, ebird.dtic.mil/Aug1999/s19990817author.htm. ("[Richard] Clarke, whose formal title is National Coordinator for Security, Infrastructure Protection and Counterterrorism, has been warning for years about the threat of an 'electronic Pearl Harbor. . . .'").

114. 323 U.S. 214 (1944).

115. *See* WILLIAM REHNQUIST, ALL THE LAWS BUT ONE: CIVIL LIBERTIES IN WARTIME 220–243 (1998).

116. *See generally*, MARTIN VAN CREVELD, TECHNOLOGY AND WAR: FROM 2000 B.C. TO THE PRESENT (1991).

117. VICTOR DAVIS HANSON, SOUL OF BATTLE: FROM ANCIENT TIMES TO THE PRESENT DAY, HOW THREE GREAT LIBERATORS VANQUISHED TYRANNY (1999).

118. U.S. Commission on National Security/21st Century, New World Coming: American Security in the 21st Century, Sept. 15, 1999, www.nssg.gov/Reports/New_World_ Coming/new_world_coming.htm.

119. *New Terrorism Vs Individual Liberties*, SAN FRANCISCO CHRONICLE, Sept. 22, 1999, at 22, ebird.dtic.mil/Sep1999/s19990923threats.htm.

120. *Id.*