CHAPTER 12

WHERE DOMESTIC SECURITY AND CIVIL LIBERTIES COLLIDE[1]

Charles J. Dunlap, Jr.

Imagine, if you will, that there was fairly hard evidence that next year a group of people would kill 40,000 Americans, injure another 6 million,[2] and inflict some $150 billion in economic losses on this country.[3] Compare that situation with a problem that last year killed or injured no one and cost, at most, some $8 billion.[4] Which one would—or should—garner the most attention of the national security community?

One would think that the military would put emphasis on the former, while the latter would be left to state or federal law enforcement personnel to sort out. Actually, the focus is much the reverse. The first set of numbers describes the annual impact of motor vehicle accidents while the second represents the combined costs of nuclear, biological, chemical, and cyber attacks on the United States. Still, some experts—many of whom once apocalyptically touted Y2K[5] perils—insist that the U.S. homeland is exceptionally vulnerable to such threats. And the U.S. military is listening. Today, it is beginning to pour resources into efforts to defend against dangers that have rarely manifested themselves not only here, but *anywhere*.

It is, of course, true that the *potential* dangers posed by weapons of mass destruction (WMD) are very great—in theory. No one disputes that we should take prudent steps to defend against them. Prudence dictates, however, a hardnosed assessment of risk so that reasonable decisions are made as to how to focus effort and allocate scarce resources. Accordingly, as we look at the many challenges facing the armed forces today, we ought to consider that during the period 1993-98 (the latest government figures available) there were only seven casualties (primarily as a result of the World Trade Center bombing) from *any* international terrorist action in North America.[6]

Nevertheless, the U.S. Government has stepped up its efforts to combat terrorism. For example, Presidential Decision Directive 62 (PDD-62) was issued in 1998. PDD-62 made fighting terrorism "a top national security objective" to be pursued with the "goal of ensuring that we meet the threat of terrorism in the 21st century with the same rigor that we have met military threats in this century."[7] Despite the rhetoric of a "national security objective," terrorism remains formally a law enforcement problem, and our official aim is to "bring terrorists to justice for their crimes."[8] Law enforcement problems are, of course, not a traditional responsibility of the uniformed services.

Clearly, not every threat to "national security" is by definition the responsibility of the armed forces. Failing schools, economic troubles, and social unrest may all imperil national security broadly construed, but it does not necessarily follow that the military should provide solutions. The courts have repeatedly held that the purpose of the armed forces is "to fight or be ready to fight wars should the occasion arise."[9] Yet the military is ever more frequently employed to confront a broader range of national ills. Why? One reason is that the military seems to get things done. In a very insightful 1991 article in *Atlantic Monthly* magazine, James Fallows wrote, "I am beginning to think that the only way the national government can get anything worthwhile done is to invent a security threat and turn the job over to the military."[10]

In my view, when what is "turned over to the military" is something that is principally a law enforcement problem, the military—and the nation—assumes risk. There are relatively few modern examples where systematic use of the military to meet internal security threats has been good for democracy or, for that matter, the military itself. As to the latter, consider the performance of the Argentine Army during the 1982 Falklands/Malvinas conflict. Argentine soldiers, who had proven themselves rather expert at torturing and killing their fellow citizens in internal security operations, were rather less effective when facing the British Army on the battlefield. The mere presence of *real* soldiers—the Gurkha Regiment and elite paratroop units—panicked many Argentine conscripts into surrender with hardly a shot fired. Internal security duties do something to military forces, and I submit it is not something good for warfighting.

But let us focus on the impact on democratic values of the regularized use of the military for policing-type duties. I believe the Founding Fathers would be rather horrified at the suggestion that the regular military forces, the "standing army" so to speak, were to be used in any systemized way for internal security. They were very cognizant of the excesses of Cromwell's New Model Army in England,[11] and resented the use of Royal troops in the colonies to suppress the growing protest against imperial rule.[12] The killing of five colonists in 1770 by the British Army still resonates as the "Boston Massacre."

From the very beginning, Americans considered a standing army a threat to liberty. They also did not like supporting troops through taxes or otherwise. In fact, the infusion of British regulars into local communities was the reason one of the least known parts of the Constitution, the Third Amendment, was later adopted. This provision—which sounds quaint to modern ears—forbids the quartering of troops in private homes without the consent of the owners. We are hardly aware of this Amendment because the military establishment has wisely avoided doing things that would awaken latent antimilitarism infringing upon Americans in their home.

To me, history teaches us that there is a form of antimilitarism deeply embedded in the American character.[13] It is usually benign, but represents a potential that today's militaries must never forget. We should keep in mind that what the architects of the Constitution really hoped was that a professional military of any size would not be required.[14] In terms of a military establishment, they conceived of one not designed for force projection but rather an organization distinctly defensive in character. It would center on a small cadre of full-time professionals who would be augmented in wartime by mustering of huge state militias. The militia system never really worked as originally envisioned, but, up until the start of the Cold War, the pattern in the United States was a small standing peacetime force that grew rapidly during conflicts through the massive addition of volunteers and conscripts.

The small size of the professional military, if nothing else, precluded much interference with the rights of American citizens during most of U.S. history. Wartime did create exceptions, but Americans generally did not like the experience. During the Civil War, for example, the military sought to exercise martial law authority.[15] In the case of *Ex Parte Milligan,*[16] a civilian—a lawyer, incidentally,—was tried by military commission for various seditious acts and sentenced to death. The Supreme Court ultimately threw out the conviction, holding that, so long as the civil courts remained open, the military could not extend its authority to civilians, even under the exigencies of national security in wartime.

One of the principal examples of the *systemized* use of the armed forces for law enforcement in peacetime was in the post-Civil War south. Again, the experience was not a good one and eventually produced legislation that today represents the principal legal impediment to the use of the military for law enforcement duties. Largely as a result of questionable activities of federal troops in response to a railroad strike and during the election of 1878,[17] Congress passed the Posse Comitatus Act.[18] That statute—which was welcomed by most military officers at the time[19]—criminalizes the use of the armed forces to execute the laws (subject to a few exceptions). As influential as it is in many situations, there has never been a conviction for violation of the Act.

Of course, troops have always been used to suppress riots and other domestic civil disorders throughout U.S. history.[20] These were mainly situations where the disturbances plainly exceeded available police resources. Perhaps the darkest, most disturbing uses of the military for internal security purposes was during the 1960s and 70s, a period made turbulent by the confluence of civil rights and antiwar protests. Professor Loch Johnson reports that, not only was the National Security Agency secretly recording every cable sent overseas by Americans for almost 30 years, “Army intelligence units conducted investigations against 100,000 Americans during the Vietnam War.”[21] A Senate investigation (the Church Committee) in the early 1970s made public for the first time the extensive scope of the military’s surveillance of U.S. citizens.[22] When the military’s activities were revealed, a plethora of legislation and other regulations followed.[23] These still limit the information the armed forces can collect on American citizens domestically. So damaging were the excesses exposed, the military’s appetite for domestic security activities dampened markedly.

By the early 1980s, however, the drug crisis in this country catalyzed Congress into passing a number of legislative initiatives to involve the armed forces in the war on drugs. [24] The United States was in the midst of a crime wave for which illegal narcotics was much to blame, and which Congress believed was overwhelming police forces. The new authorities still restricted the military from engaging in direct law enforcement activities, such as search and seizure, and arrests—but they did permit the provision of training, equipment, and specialized technical services. The nearly 2-decade effort has cost billions and involves even today thousands of soldiers, sailors, and airmen. As will be discussed below, these activities can be controversial.

Today, we see fears of terrorism against homeland targets fueling a renewed effort to involve the military in domestic security. This is especially true with respect to cyberterrorism. In May of 1998 Presidential Decision Directive (PDD) 63[25] was issued which sets out a blueprint to expand the role of the Department of Defense (DoD) in countering cyber terrorism. Specifically, DoD is listed as the "lead agency" in the area of "national defense."[26] As such, DoD is "coordinating all of the activities of the United States Government in that area."[27] PDD 63 does not, however, define the parameters of "national defense,"[28] an especially problematic situation given the dual-use (i.e., used by both military and civilian persons) nature of many of the systems subject to cyber assaults. How can DoD escape intruding into civilian areas with such a loosely defined mission?

Other steps also have been taken just in the last year or so. Notwithstanding the withering criticism of the National Security Agency (NSA) by the Church Committee in the 1970s, DoD has assumed an "information assurance mission."[29] According to its own public documents, it "conducts defensive information operations, to achieve information assurance for information infrastructures critical to U.S. national security interests."[30] Towards the end of 1998, DoD also established Joint Task Force Computer Network Defense (JTF-CND)[31] and tasked it to coordinate the defense of all DoD computer systems.[32] In October 1999 JTF-CND,[33] along with the Joint Information Operations Center was placed under the control of U.S. Space Command (USSPACECOM). In a separate project, DoD established the Defense Computer Forensics Lab in September of 1999.[34] Among other things, the lab seeks to chase across the Internet hackers who assault DoD systems.[35]

Not all of the recent effort has focused exclusively on defending against domestic cyber attacks. After discussion of the establishment of a "Homeland Defense" command was aborted when civil libertarians complained, DoD established Joint Task Force-Civil Support (JTF-CS).

JTF-CS has a relatively uncontentious charter that merely tasks it to assist civilian authorities in “consequence management,” that is, dealing with the after effects of a catastrophe, regardless of its source, but most likely the result of terrorism involving WMD, 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.[36]

Parenthetically, it seems to make sense that many of these homeland defense missions would default to the National Guard. Conceptually, such a mission would appear to fit with the traditional, local orientation of the Guard. Moreover, its historical citizen-soldier model should temper public concerns about an overreaching “standing army.” In a way, however, Total Force has been too successful. With fewer and fewer members of the public showing any military experience in their resumes, the average citizen perceives no differences among those persons in uniform. Everyone—regardless of component—is, for example, “the Army” in a corporate sense to the proverbial “man in the street.”

Accordingly, any improper action by one component will probably be imputed to all. Another Kent State shooting will undermine the reputation of the Regular Army, notwithstanding that the Reserves or Guard might have committed the act. Thus, it is unlikely that designating a Guard officer as the JTF-CS commander as opposed to an officer from another component will have any real ameliorating effect on potential civil-military relations friction. It may even have an aggravating effect because the Guard (and to a lesser extent the Reserves) has no tradition of being apolitical. The openly political behavior of some in the Guard carries great potential to create tensions between the armed forces and the citizenry if the trend towards greater involvement in law enforcement activities persists.

Why is the use of armed forces as an internal security tool considered so suspect by civil libertarians and others? Secretary of Defense William Cohen captured a key issue, when speaking about the frustrations of the Army's attempts to police areas in Kosovo, commented in January 2000 that the Army is "not trained for that; they are not competent really to carry out police work, nor should they be doing it."[37] Cohen is right, but not just in the Kosovo context. From the constabulary peacekeeping missions of the 1990s, we learned that the skills of the combat soldier are not necessarily coterminous with those of the policeman.

Although this should be intuitive, many uniformed people fail to sufficiently appreciate that there are fundamental differences and, I would submit, *incompatibilities* between the *culture* of the soldier and culture of the policeman. One could almost say that the mental wiring is different. For example, it always amazes me that some officers believe that their oath to "support and defend" the Constitution against "all enemies, foreign and domestic"[38] is somehow license (if not duty) to engage in domestic law enforcement activities. It is as if they believe that persons suspected of crimes are somehow domestic "enemies" of the state. Of course, under our system of law, those accused of crimes are *innocent* persons until proven otherwise in a court of law—not enemies of the state, domestic or otherwise. But military people are oriented to think of adversaries as enemies, not as suspects entitled to the presumption of innocence.

This difference in thought patterns manifests itself in other ways as well. Members of the armed forces think of power in brute, physical terms: mass, weight of effort, rates of fire, and so forth. A law enforcement officer draws his power not from his weaponry *per se*, but from moral authority his status and position in society exerts. It interesting to note that experts are starting to realize that the militarization of the police in the past two decades, that is, their tendency to ape military organizations through SWAT units, heavier weapons, body armor, and so forth, may well be counterproductive. Such factors undermine their effectiveness by creating a new mindset based on *physical* power that diminishes their moral authority. In discussing the explosion in the number of disturbing incidents across the country of heavy-handed police behavior, former police chief John McNamara admitted recently that "some corrosive assumptions [have] crept into police culture."[39] He says,

> The fundamental duty of police is to protect human life. But in many places that understanding has been superseded by a militaristic approach, one that allows for an acceptable number of casualties and that views much of the population as hostile.[40]

Military authorities ought to take note of the problems that a "militaristic approach" generates. Moreover, just as some in the armed forces tend to perceive American citizens suspected of crimes as "enemies" of the state, military members can also evaluate threats very differently than do properly-focused and trained law enforcement personnel. Consider the 1997 shooting of a Texas teenage shepherd by a Marine Corps border surveillance patrol. The youngster (who was probably unaware of the camouflaged military presence) may simply have been casually shooting at game as he tended his flock, but the Marines seem to have mistook this as fire being directed against them, and responded with deadly force. A policeman faced with a threat may well retreat and contain a situation out of concern not only for himself and other innocents, but also for the safety of the "threat" itself. But a military person thinks of destroying threats, not keeping them safe for arrest and judicial disposition, and this may have been a factor in the Texas shooting.

Consider this mindset in the cyberterrorism context. If you do, it should be no surprise—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."[41] In responding to the report's proposal to allow the military to immediately launch an electronic 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?"[42] I hope not, but maybe.

Furthermore, the threat of cyberterrorism is generating calls from some to abandon the policy that limits the use of the military's intelligence gathering and other resources against domestic cyber-incidents. U.S. policy today assumes that, absent evidence to the contrary, cyber assaults involve U.S. persons. The presumption of a "U.S. person" means that it is thus first and foremost a law enforcement matter. This ensures that the judicial process is used in the event intrusion into the citizenry is required in the course of the investigation. It also greatly limits the involvement of the military, and especially its intelligence gathering assets. The new proposals call for a revised policy that presumes the digital "intruder is *not* a U.S. person," thus permitting "the full capabilities of the United States' investigative and intelligence assets" to be "brought to bear" as some desire.[43] Legislation allowing the military and other intelligence agencies to investigate U.S. citizens is currently under consideration.

I believe such proposals are often welcomed within the military establishment (and even outside of it) because it is not well appreciated exactly why the armed forces represents a far greater threat to civil liberties than do even the most robust law enforcement organizations. The genius of the American scheme of law enforcement organization from a civil liberties perspective is that the power represented by more than 780,000 sworn officers is diffused into over 18,000 independent or semi-independent police forces subject to local control. If a particular agency runs amok, there is ample counterbalance available. There is really no similar counterbalance to the U.S. military establishment. This is not much of a concern so long as the armed forces remains *externally* focused—the threat to rights at home is minimized. But no such assurance can be made once the physical power, mental energy, and organizational unity of the armed forces turns inward toward the American citizenry itself.

Nevertheless, the military *must* turn inward *if* the threat to homeland security is such that existing law enforcement agencies are incapable of dealing with it. We must recognize that if that occurs, civil liberties are almost certain to be at risk. In 1997 Secretary of Defense Cohen admitted,

> terrorism is escalating to the point that citizens of the United States may soon have to choose between civil liberties and more intrusive forms of protection.[44]

The "more intrusive form of protection" could, of course, involve the military.

The armed forces certainly have a role to play in confronting terrorism, but not necessarily an intrusive one. In the short term, I believe that the military's role in consequence management is a necessary one—there really is no option in the case of a cataclysmic nuclear, biological, or chemical attack. While it may be wise to build and equip the necessary consequence management organizations in the civilian sector as is currently underway, it seems to me that the episodic nature of such events, as well as the limited scope of the military's role, makes the risk to civil liberties manageable.

I am much more concerned about the use of the military to confront the threat of cyberterrorism. The invasive nature of cyber investigations, as well as the technical difficulty of determining the origin of cyber attacks, almost by definition will result in military confrontations with U.S. citizens, many of whom will be innocent of any offense. The key question is whether or not military involvement is really warranted by the threat. In my view, it is not. I believe that all the dour predictions that a teenager with a Palm Pilot could hack New York into darkness are wildly overblown.

Writing in the winter issue of *Foreign Policy*,[45] cyberwar expert Martin Libicki asserts that conducting a truly meaningful attack on critical computer systems is far more difficult than popular wisdom suggests. Libicki points out that if it were really as cheap and as easy to do as so many cyberzealots claim, someone, somewhere, would have done it already. Countering this view, Professor Dan Kuehl of the National Defense University testified before Congress in February on this issue. He said 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."[46]

I do not share Professor Kuehl's view. There are too many actors out there—Slobodan Milosevic, Saddam Hussein, Osama bin Laden, and many others—who would surely hurt the United States *if they could*, especially if they could do so anonymously as the cyberzealots insist is possible. Looking beyond our borders, does anyone seriously believe that Chechens would refrain from launching a devastating computer attack against Russia? Would they see no "strategic advantage" in doing so, even though their country is being demolished and their people slaughtered by Russian troops? What about the Kurds suffering in Iraq? Or Turkey? How about the IRA against Britain?

The idea that *all* of these different groups would come to precisely the same strategic conclusion to "desist" *vis-à-vis all* these potential targets despite profound cultural differences simply strains credibility too far. The real reason crippling attacks have not taken place is that it is just too hard to do—and getting harder every day as the financial rewards of e-commerce are stimulating vast expenditures for net security. Keep in mind that I am not talking about denial-of-service attacks[47] that close down a commercial web site for a couple of hours[48]—that should not be a military concern—I'm talking about taking down the nation's critical infrastructures for a significant period.

Does this mean that serious and costly cyber incidents will *never* occur? No. It merely means that there is insufficient evidence today to require a *military* role in the law enforcement aspects. Even a hugely tragic incident involving thousands of deaths and billions in damage are no more of a risk—and no more beyond the abilities of traditional law enforcement entities to address—than are, as previously discussed, the motor vehicle accidents we suffer every year or, for that matter, the World Trade Center or Oklahoma City bombings. We should recall that Martin Van Creveld maintains terrorism has not succeeded in developed states because modernity itself produces redundancies and work-arounds that rapidly mitigate even savage attacks.[49] Cyberterrorism cannot bring America to its knees.

The military ought to get involved in homeland cyberdefense when it becomes apparent that some opponent has a genuine capability to inflict losses extensive enough to truly *cripple* critical military or civilian systems in such a way as to really harm to our vital interests and threaten our way of life. I do not believe such proof exists. Nevertheless, our military and civilian leaders repeatedly insist we are vulnerable to an "electronic Pearl Harbor."[50] Using the rhetoric of the infamous sneak attack is a clever way to shock people into supporting the kind of civil liberty compromises about which Secretary Cohen spoke.

To me, however, Pearl Harbor suggests other images. They are scenes of U.S. Army troops herding loyal citizens into barb-wired detention camps because of rhetoric about a threat that in reality was nonexistent. Although it may be fashionable today to say that racism explains the treatment of Japanese-Americans in the wake of Pearl Harbor, the reality is much different. A careful reading of the Supreme

Court's decision in *Korematsu v. United States*,[51] reveals that honorable men in the embrace of genuine—albeit wildly mistaken—fears made the decision to incarcerate hundreds of thousands of equally honorable American citizens. That said, we should learn from this history the *real* danger to American values posed by overestimation of the dangers we face.

As we calculate the risks of an enhanced role for the military in homeland defense, we should recall that the damaging revelations of the Church Committee in the early 1970s heralded a post-Vietnam downward slide for the Army and the military in general. After an enormous effort in the late 1970s and 1980s, the U.S. armed forces emerged to become what is today the most trusted institution in American society. [52] Yet we seem to have forgotten the lessons of the past. I am absolutely convinced that a deepening involvement of the armed forces in any kind of domestic activity associated with law enforcement or investigations carries great potential to re-ignite the anti-militarism that is never far from the surface of the American psyche. The huge controversy over the alleged role of military in the fiery conclusion of David Koresh's standoff with Federal authorities at Waco, Texas, should serve as a warning in this regard. In an era when the armed forces are already struggling to recruit and retain the best and brightest, a loss of public confidence and trust would be a *real* catastrophe.

Finally, I'm convinced that terrorists can cause more harm to our way of life by forcing us to give up our civil liberties than they can by the actual damage they might do. The *San Francisco Chronicle* made this point in an editorial where it reported 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.[53]

It wisely counseled that "it is better to live with danger than in the security of a police state."[54] I believe that most Americans share that view, and it ought to shape the military's response as we consider the U.S.'s homeland defense policies.

CHAPTER 12 - ENDNOTES

1. Elements of this presentation were drawn from *Meeting the Challenge of Cyberterrorism: Defining the Military Role in a Democracy*, Paper presented by the author at the Symposium on Cyberterrorism: "The World Held Hostage in the Digital Age," Villanova University School of Law,Villanova, PA, March 18, 2000 (copy on file with the author). A version of that presentation will be published by the Naval War College in Fall 2000.

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

3. *See* National Highway Traffic Safety Administration, *The Economic Cost of Motor Vehicle Crashes, 1994* (1995) Internet *http://www.nhtsa.dot.gov/people/economic/ecomvc1994.html* (accessed March 15, 2000).

4. John J. Stanton, "Rules Of Cyberwar Baffle U.S. Government Agencies," *National Defense*, February 2000, Internet *http://ebird.dtic.mil/Feb2000/s20000208rules.htm* (accessed March 15, 2000).

5. "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 DoD program to address Y2K, *see http://www.defenselink.mil/issues/y2k.html* (accessed March 15, 2000).

6. U.S. Department of State, Office of the Coordinator for Counterterrorism, "Total International Casualties by Region 1993-1998," in *Patterns of Global Terrorism 1998* (1999) Internet *http://www.state.gov/www/global/terrorism/1998Report/r.gif* (accessed April 11, 2000).

7. *See* The White House, Office of the Press Secretary, *Combating Terrorism: Presidential Decision Directive 62*, May 22, 1998 (Fact Sheet), Internet *http://www.pub.Whitehouse.Gov/uri-res/*

I2R?urn:pdi:/ /oma.eop.gov.us/1998/5/22/7.text.1 (accessed April 11, 2000).

8. U.S. Department of State, Office of the Coordinator for Counterterrorism, *U.S. Counterterrorism Policy*, Internet *http://www.state.gov/www/global/terrorism/index.html* (accessed April 11, 2000).

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

10. James Fallows, "Military Efficiency," *The Atlantic Monthly*, August 1991, p. 18.

11. See, generally, William S. Fields & David Hardy, "The Militia and the Constitution: A Legal History," *Military Law Review*, Vol. 1, No. 136, 1992, pp. 9-13; see also Caleb Carr, "The Troubled Genius of Oliver Cromwell," *Military History Quarterly*, Summer 1990, p. 82.

12. See, generally, Fields and Hardy, pp. 25-26.

13. *See* Charles J. Dunlap, Jr., "Welcome to the Junta: The Erosion of Civilian Control of the U.S. Military," *Wake Forest Law Review*, Vol. 29, No. 341, Summer 1994, pp. 342-354.

14. See, generally, Fields and Hardy, pp. 9-13; see also Carr, p. 82.

15. See, generally, Charles Fairman, *Martial Law*, Chicago: Callaghan and Company, 1943, pp. 108-116.

16. 71 U.S. 2, 1866.

17. Stephen Dycus, Arthur L. Berney, William C. Banks, and Peter Raven-Hansen, *National Security Law*, New York: Little, Brown and Company, 1990, p. 427.

18. Act of June 18, 1878, ch. 263, § 15, 20 Stat. 152 (current version at 18 U.S.C. § 1385 (Supp. 1999)).

19. Jerry Cooper, "The Posse Comitatus Act," in John Whiteclay Chambers, II, ed., *The Oxford Companion to American Military History*, 1999, pp. 555-556.

20. See, generally, David E. Engdahl, *Soldiers, Riots, and Revolution: The Law and History of Military Troops in Civil Disorders*, 57 Iowa Law Rev. 1, October 1971.

21. Loch K. Johnson, *A Season of Inquiry*, 1985, p. 223.

22. See, generally, *Ibid.*

23. See, for example, Foreign Intelligence Act of 1978, 50 U.S.C.A. §§ 1801-1811, 1991; and Exec. Order No. 12,333, 46 Fed. Reg. 59,941, 1981 (limiting, *inter alia*, the use of intelligence agencies including those of the armed forces to collect information on persons within the United States).

24. See, for example, 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 U.S.C. § 371-380 (1988).

25. 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 *http://www.pub.whitehouse.gov/uri-res/ I2R?urn:pdi: // oma.eop.gov.us/ 1998/5/26/1.text.1* (accessed March 12, 2000).

26. *Ibid.*, pp. 4, 8.

27. *Ibid.*

28. The Navy has the Fleet Information Warfare Center web site available at *http://www.fiwc.navy.mil/html/home.html*, (accessed March 12, 2000), and the Army has the Information Assurance Directorate web site available at *http://www.army.mil/ disc4/isec/c2p/mission/mission.htm* (accessed March 12, 2000).

29. National Security Agency, *Mission Statement*, available at *http://www.nsa.gov/about_nsa/mission.html* (accessed April 16, 2000).

30. *Ibid*.

31. Office of the Assistant Secretary of Defense (Public Affairs), *Joint Task Force On Computer Network Defense Now Operational*, December 30, 1998, (press release) available at *http://www. defenselink.mil/news/Dec1998/b12301998_bt658-98.html* (accessed March 15, 2000).

32. *See* Frank Wolfe, "Joint Task Force To Direct Pentagon's Cyber Defense," *Defense Daily*, January 26, 1999, p. 1, available at *http://ebird.dtic.mil/Jan1999/e19990126joint.htm* (accessed March 15, 2000).

33. U.S. Space Command, *USSPACECOM Takes Charge of DoD Computer Network Defenses*, Release No. 19-99, October 1, 1999 (press release) available at *http://www.spacecom.af.mil/usspace/new19-99.htm* (accessed March 15, 2000).

34. Douglas J. Gilbert, *High-Tech Lab Ties Computers to Crimes*, American Forces Press Service, November 1999, available at *http://www.defenselink.mil/news/Nov1999/n11021999_9911023.html* (accessed March 15, 2000).

35. *Ibid.*

36. Linda D. Kozaryn, *DoD Helps Hometown USA Confront Terrorism*, American Forces Press Service, January 2000, available at *http://www.defenselink.mil/news/Jan2000/n01132000_20001133.html* (accessed March 16, 2000).

37. Department of Defense, News Briefing, *Secretary of Defense William S. Cohen and Secretary of State for Defense Geoffrey Hoon*, January 27, 2000 (quoting William S. Cohen) available at *http://www.defenselink.mil/news/Jan2000/t01272000_t0027uk_.html* (accessed March 30, 2000).

38. 5 U.S.C.A. § 3331 (West 1996).

39. Ellis Close, "Cracks in the Thin Blue Line," *Newsweek*, April 10, 2000, p. 33 (quoting John McNamara).

40. *Ibid.*

41. *See* Bob Brewin, "Report: Allow Cyberwar Response," *Federal Computer Week*, March 29, 1999 (citing a report by the National Resource Council), available at *http://www.fcw.com/fcw/articles/1999/FCW_032999_255.asp* (accessed March 15, 2000).

42. *Ibid.*

43. Walter Gary Sharp, Sr., "Balancing Our Civil Liberties with Our National Security Interests in Cyberspace," *Texas Review Law and Policy*, Vol. 4, No. 69, 1999, pp. 72-73 (emphasis in the original).

44. As quoted in Patrick Pexton, "Banking on a Revolution," *Air Force Times*, September 22, 1997, p. 3.

45. Martin Libicki, "Rethinking War: The Mouse's New Roar?," *Foreign Policy*, Winter 1999/2000, p. 30. Abstract available at

http://www.foreignpolicy.com/articles/winter1999-2000/Libicki.htm (accessed March 14, 2000).

46. Vernon Loeb, "Cyberwar's Economic Threat," *The Washington Post*, February 24, 2000, p. 19, quoting Dan Kuehl.

47. See, for example, Brendan I Koerner, "The Web's Bad Week," *U.S. News & World Report*, February 21, 2000, p. 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.")

48. See Anne Plummer, "Pentagon Response To Commercial Denial-of Service Attacks Limited," *Defense Information and Electronics Report*, February 18, 2000, p. 1 (describing the denial of service attacks in early 2000 as "little more than criminal mischief").

49. See, generally, Martin Van Creveld, *Technology and War: From 2000 B.C. to the Present* (revised and expanded edition), 1991, pp. 305-306.

50. See Jim Garamone, *Hamre "Cuts" Op Center Ribbon, Thanks Cyberwarriors*, American Forces Information Services, August 1999, available at *http://www.defenselink.mil/news/Aug1999/n08241999_9908241.html* (accessed March 11, 2000), quoting Deputy Defense Secretary Hamre ("Several times I've testified and talked about the future electronic Pearl Harbor to the United States").

51. 323 U.S. 214 (1944).

52. Sixty-eight percent of Americans said they had "a great deal" or "quite a lot" of confidence in the military. Organized religion was second at 58 percent. The Presidency and Congress were reported at 49 and 26 percent, respectively. See Tamar A. Mehuron, "Military First in Public Confidence," *Air Force Magazine*, March 2000, p. 9 (citing a late 1999 Gallup poll), available at *http://www.afa.org/magazine/chart/0300chart.html* (accessed April 5, 2000).

53. "New Terrorism Vs Individual Liberties," *San Francisco Chronicle*, September 22, 1999, p. 22, available at *http://ebird.dtic.mil/Sep1999/s19990923threats.htm* (accessed March 15, 2000).

54. *Ibid.*